AWS Whitepaper

Connettività ibrida

Connettività ibrida: AWS Whitepaper

Table of Contents

Connettività ibrida

Data di pubblicazione: 6 luglio 2023 (Revisioni del documento)

Molte organizzazioni devono connettere i data center locali, i siti remoti e il cloud. Una rete ibrida collega questi diversi ambienti. Questo white paper descrive gli elementi costitutivi di AWS e i requisiti chiave da considerare per decidere quale modello di connettività ibrida è giusto per te. Per aiutarti a determinare la soluzione migliore per i tuoi requisiti aziendali e tecnici, forniamo alberi decisionali che ti guidano attraverso il processo di selezione logica.

Introduzione

Un'organizzazione moderna utilizza una vasta gamma di risorse IT. In passato, era comune ospitare queste risorse in un data center locale o in una struttura di colocation. Con la crescente adozione del cloud computing, le organizzazioni forniscono e utilizzano le risorse IT dei provider di servizi cloud tramite una connessione di rete. Le organizzazioni possono scegliere di migrare alcune o tutte le risorse IT esistenti sul cloud. In entrambi i casi, è necessaria una rete comune per connettere le risorse locali e cloud. La coesistenza di risorse locali e cloud si chiama cloud ibrido e la rete comune che le collega viene definita rete ibrida. Anche se l'organizzazione mantiene tutte le risorse IT nel cloud, potrebbe comunque richiedere la connettività ibrida ai siti remoti.

Esistono diversi modelli di connettività tra cui scegliere. La disponibilità di opzioni aumenta la flessibilità, ma la selezione dell'opzione ottimale richiede l'analisi dei requisiti aziendali e tecnici e l'eliminazione delle opzioni non adatte. È possibile raggruppare i requisiti in base a considerazioni quali sicurezza, tempi di implementazione, prestazioni, affidabilità, modello di comunicazione, scalabilità e altro ancora. Dopo aver raccolto, analizzato e considerato attentamente i requisiti, gli architetti di rete e cloud possono identificare gli elementi costitutivi e le soluzioni di rete AWS ibrida applicabili. Per identificare e selezionare il modello o i modelli ottimali, gli architetti devono comprendere i vantaggi e gli svantaggi di ciascun modello. Esistono anche limitazioni tecniche che potrebbero causare l'esclusione di un modello altrimenti adatto.

Per semplificare il processo di selezione, questo white paper illustra ogni considerazione chiave in un ordine logico. Per ogni considerazione, ci sono domande utilizzate per raccogliere i requisiti. Viene identificato l'impatto di ogni decisione di progettazione, insieme alle potenziali soluzioni. Il white paper presenta gli alberi decisionali relativi ad alcune considerazioni come metodo per facilitare il processo decisionale, eliminare le opzioni e comprendere le conseguenze di ogni decisione. Si conclude con uno scenario che copre un caso d'uso ibrido, applicando la selezione e la progettazione del end-

to-end modello di connettività. È possibile utilizzare questo esempio per vedere come eseguire i processi descritti in questo white paper in un esempio pratico.

Questo white paper ha lo scopo di aiutarti a selezionare e progettare un modello di connettività ibrida ottimale. Questo white paper è strutturato come segue:

- Elementi fondamentali della connettività ibrida: una panoramica dei AWS servizi utilizzati per la connettività ibrida.
- Considerazioni sulla selezione e sulla progettazione della connettività: una definizione di ciascun modello di connettività, il modo in cui ciascuno influisce sulla decisione di progettazione, le domande di identificazione dei requisiti, le soluzioni e gli alberi decisionali.
- Un caso d'uso per un cliente: un esempio di come applicare in pratica le considerazioni e gli alberi decisionali.

Sei tu Well-Architected?

Il AWSWell-Architected Framework ti aiuta a comprendere i pro e i contro delle decisioni che prendi quando crei sistemi nel cloud. I sei pilastri del Framework consentono di apprendere le migliori pratiche architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili. Utilizzando AWS Well-Architected Tool, disponibile gratuitamente in AWS Management Console, puoi esaminare i tuoi carichi di lavoro rispetto a queste best practice rispondendo a una serie di domande per ogni pilastro.

Per ulteriori indicazioni e best practice da parte degli esperti per la tua architettura cloud (implementazioni dell'architettura di riferimento, diagrammi e white paper), consulta l'Architecture Center. AWS

AWSelementi costitutivi della connettività ibrida

Esistono tre elementi costitutivi di un'architettura di connettività di rete ibrida:

- Connessioni di rete ibride: i tipi di connessione tra i servizi di AWS connettività e i dispositivi gateway del cliente locali.
- AWSservizi di connettività ibrida: i AWS servizi che forniscono connettività e routing tra l'infrastruttura del cliente e. AWS
- Dispositivo gateway del cliente locale: il dispositivo all'interno della rete esistente del cliente che rappresenta l'endpoint locale per la connessione di rete ibrida. Tipi di connessione diversi hanno requisiti tecnici diversi per questi dispositivi, descritti nelle sezioni seguenti.

Connessioni di rete ibride

Esistono diversi modi per connettersi tra le proprie apparecchiature locali ad. AWS Questo white paper si concentra su come questi diversi modi possono essere combinati in architetture generali, tuttavia viene fornita una breve panoramica delle diverse opzioni (AWS Direct Connectrete privata virtuale da sito a sito e Transit Gateway Connect).

AWS Direct Connect

AWS Direct Connectè un servizio che stabilisce una connessione di rete dedicata dalle proprie sedi adAWS. Per informazioni dettagliate, consulta AWS Direct Connect.

Esistono due tipi di AWS Direct Connect connessioni: dedicate e ospitate. Una connessione dedicata è un collegamento diretto tra un AWS dispositivo e il dispositivo locale, mentre una connessione ospitata è supportata da un AWS partner che può gestire i dettagli della connessione per te. Per ulteriori informazioni, consulta le AWS Direct Connectconnessioni.

Una connessione Direct Connect utilizza interfacce virtuali (VIF) per isolare diversi flussi di traffico. Più VIF possono utilizzare lo stesso collegamento Direct Connect, separato da tag VLAN (802.1q). Esistono tre tipi di VIF che forniscono connettività alla rete. AWS Vedi le interfacce AWS Direct Connect virtuali per maggiori dettagli. I tre tipi sono:

- VIF privata: una VIF privata è una connessione privata tra il dispositivo e le risorse interne. AWS Questi terminano all'interno direttamente AWS su un Virtual Private Gateway (VGW) (che supporta un singolo VPC) o tramite un Direct Connect Gateway che poi si connette a più VGW.

- VIF pubblico: un VIF pubblico consente la connettività a qualsiasi AWS risorsa pubblica, come S3, DynamoDB e intervalli IP EC2 pubblici. Sebbene un VIF pubblico non abbia accesso diretto a Internet, qualsiasi risorsa pubblica di Amazon può raggiungerlo (comprese le istanze EC2 pubbliche di altri clienti), cosa che i clienti dovrebbero prendere in considerazione durante la pianificazione della sicurezza.
- Transit VIF: un Transit VIF è una connessione privata tra il dispositivo e un gateway AWS Transit Gateway Direct Connect. I Transit VIF sono ora supportati su collegamenti con velocità inferiori a 1 Gbps: consulta l'annuncio di lancio per i dettagli.

> **Note**
>
> Hosted Virtual Interface (Hosted VIF) è un tipo di VIF privato in cui il VIF è assegnato a una persona Account AWS diversa da quella proprietaria della AWS Direct Connect connessione (Account AWSche può includere un partner). AWS Direct Connect AWSnon consente più ai nuovi partner di offrire questo modello. Per ulteriori informazioni, vedere Creazione di un'interfaccia virtuale ospitata.

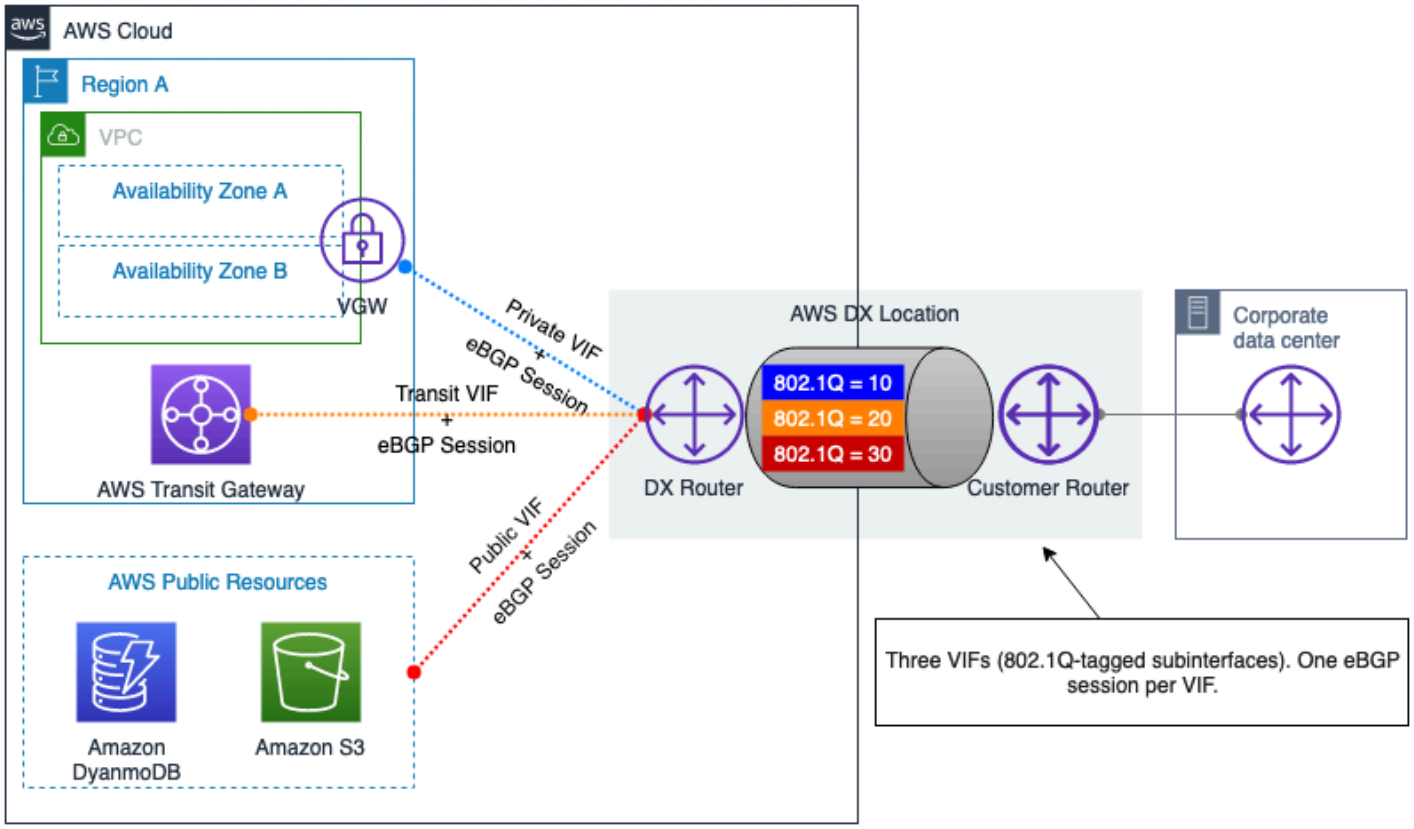

Figura 1 — VIF AWS Direct Connect private e pubbliche

Rete privata virtuale (VPN) da sito ad sito

Una site-to-site VPN consente a due reti di comunicare in modo sicuro e può essere utilizzata su un mezzo di trasporto non affidabile, come Internet. I clienti possono stabilire connessioni VPN tra siti locali e Amazon Virtual Private Clouds (Amazon VPC) tramite due opzioni:

- AWSVPN gestita da sito a sito AWS (VPN S2S): si tratta di un servizio VPN completamente gestito e ad alta disponibilità, che utilizza IPSec. Vedi Cos'è per ulteriori informazioni. AWS Site-to-Site VPN Facoltativamente puoi abilitare l'accelerazione per la connessione Site-to-Site VPN. Per ulteriori informazioni, consulta Connessioni VPN accelerate da sito ad sito. S2S VPN può anche utilizzare le VIF di transito Direct Connect per evitare che il traffico attraversi Internet, abbassando i costi e consentendo l'uso di indirizzi IP privati. Per i dettagli, consulta Private IP VPN with. AWS Direct Connect
- VPN software da sito a sito (VPN gestita dal cliente): con questa opzione di connettività VPN, sei responsabile del provisioning e della gestione dell'intera soluzione VPN, in genere eseguendo il software VPN su un'istanza EC2. Per ulteriori informazioni, consulta Software Site-to-Site VPN.

Entrambe le opzioni richiedono l'assistenza sul dispositivo gateway del cliente per chiudere l'estremità locale dei tunnel VPN. Questo dispositivo può essere un dispositivo fisico o un dispositivo software. Per ulteriori informazioni sui dispositivi di rete testati daAWS, consulta l'elenco dei dispositivi gateway dei clienti testati.

Transit Gateway Connect (TGW Connect)

Transit Gateway Connect utilizza tunnel GRE tra un dispositivo gateway locale AWS Transit Gateway e uno locale. BGP viene utilizzato in aggiunta a TGW Connect per abilitare il routing dinamico. Tieni presente che TGW Connect non è crittografato. Per ulteriori informazioni, vedere Transit Gateway Connect.

AWSservizi di connettività ibrida

AWSi servizi di connettività ibrida forniscono componenti di rete altamente scalabili e altamente disponibili. Svolgono un ruolo essenziale nella creazione di soluzioni di rete ibride. Al momento della stesura di questo white paper, esistono tre endpoint di servizio principali:

- AWSVirtual Private Gateway (VGW) è un servizio regionale altamente ridondante che fornisce il routing e l'inoltro IP a livello di VPC, fungendo da gateway per la comunicazione del VPC con i dispositivi gateway dei clienti. VGW può interrompere le connessioni VPN S2S e le VIF private. AWS AWS Direct Connect
- AWS Transit Gateway(TGW) è un servizio regionale, altamente disponibile e scalabile che consente di connettere più VPC tra loro, nonché le reti locali tramite VPN Site-to-Site e/o Direct Connect utilizzando un unico gateway centralizzato. Concettualmente, un AWS Transit Gateway funge da router cloud virtuale ridondante e altamente disponibile. AWS Transit Gatewaysupporta il routing Equal Cost Multi-Path (ECMP) su più connessioni Direct Connect, tunnel VPN o peer TGW Connect. I Transit Gateway possono collegarsi tra loro, sia nella stessa regione che tra regioni diverse, permettendo alle risorse connesse di comunicare tramite i link di peering. Per ulteriori dettagli, consulta AWS Transit Gatewaygli scenari.
- Cloud AWSLa WAN fornisce una dashboard centrale per stabilire connessioni tra filiali, data center e Amazon VPC, creando una rete globale con pochi clic. Utilizzi le policy di rete per automatizzare la gestione della rete e le attività di sicurezza in un'unica posizione. Per ulteriori dettagli, consulta la documentazione Cloud AWS WAN.
- Direct Connect Gateway (DXGW) è un servizio disponibile a livello globale che distribuisce le informazioni di routing attraverso le sue connessioni, comportandosi in modo simile ai riflettori di routing BGP in una rete tradizionale. I dati non passano attraverso un DXGW: gestisce solo le informazioni di routing. È possibile creare un DXGW in qualsiasi formato Regione AWS e accedervi da tutti gli altri. Regioni AWS È possibile collegare Direct Connect VIF a un DXGW, quindi associare il DXGW a VGW (utilizzando VIF private) o a un (utilizzando VIF di transito). AWS Transit Gateway Per ulteriori informazioni, consulta i gateway Direct Connect. Non è necessario creare più DXGW per la ridondanza in quanto si tratta di un servizio disponibile a livello globale. Tuttavia, potresti scegliere di utilizzare più DxGW per separare i domini di routing, ad esempio una rete di produzione e una di test che desideri mantenere completamente isolate.

Considerazioni sul tipo e sulla progettazione della connettività ibrida

Questa sezione del white paper illustra le considerazioni che influiscono sulle scelte effettuate nella scelta di una rete ibrida a cui connettere gli ambienti locali. AWS Segue un processo logico per supportarvi nella scelta di una soluzione di connettività ibrida ottimale. Le considerazioni che influiscono sulla progettazione sono suddivise in considerazioni che influiscono sul tipo di connettività e considerazioni che influiscono sulla progettazione della connettività. Le considerazioni sul tipo di connettività ti aiuteranno a decidere se utilizzare una VPN basata su Internet o Direct Connect. Le considerazioni sulla progettazione della connettività ti aiuteranno a decidere come configurare le connessioni.

Vengono trattate le seguenti considerazioni che influiscono sul tipo di connettività: tempi di implementazione, sicurezza, SLA, prestazioni e costi. Dopo aver esaminato queste considerazioni e il modo in cui influiscono sulle scelte di progettazione, sarete in grado di decidere se utilizzare una connessione basata su Internet o Direct Connect è consigliato per soddisfare i vostri requisiti.

Vengono trattate le seguenti considerazioni che influiscono sulla progettazione della connettività: scalabilità, modello di comunicazione, affidabilità e integrazione SD-WAN di terze parti. Dopo aver esaminato queste considerazioni e il modo in cui influiscono sulle scelte di progettazione, sarete in grado di decidere la progettazione logica ottimale consigliata per soddisfare i vostri requisiti.

La struttura seguente viene utilizzata per discutere e analizzare ciascuna delle considerazioni relative alla selezione e alla progettazione:

- Definizione - Breve definizione di ciò che è la considerazione.
- Domande chiave: fornisce una serie di domande che consentono di raccogliere i requisiti associati alla considerazione.
- Capacità da considerare: soluzioni per soddisfare i requisiti associati alla considerazione.
- Albero decisionale: per alcune considerazioni o un gruppo di considerazioni, viene fornito un albero decisionale per aiutarti a selezionare la soluzione di rete ibrida ottimale.

Le considerazioni relative alla progettazione della rete ibrida sono illustrate in un ordine in cui l'output di una considerazione fa parte dell'input per la considerazione successiva. Come illustrato nella Figura 2, il primo passaggio consiste nel decidere il tipo di connettività, per poi perfezionarlo con le considerazioni relative alla selezione del progetto.

La Figura 2 illustra le due categorie di considerazioni, le singole considerazioni e l'ordine logico in cui le considerazioni sono trattate nelle sottosezioni successive. Queste sono le considerazioni essenziali quando si prende una decisione sulla progettazione di una rete ibrida. Se la progettazione mirata non richiede tutte queste considerazioni, potete concentrarvi sulle considerazioni che si applicano ai vostri requisiti.

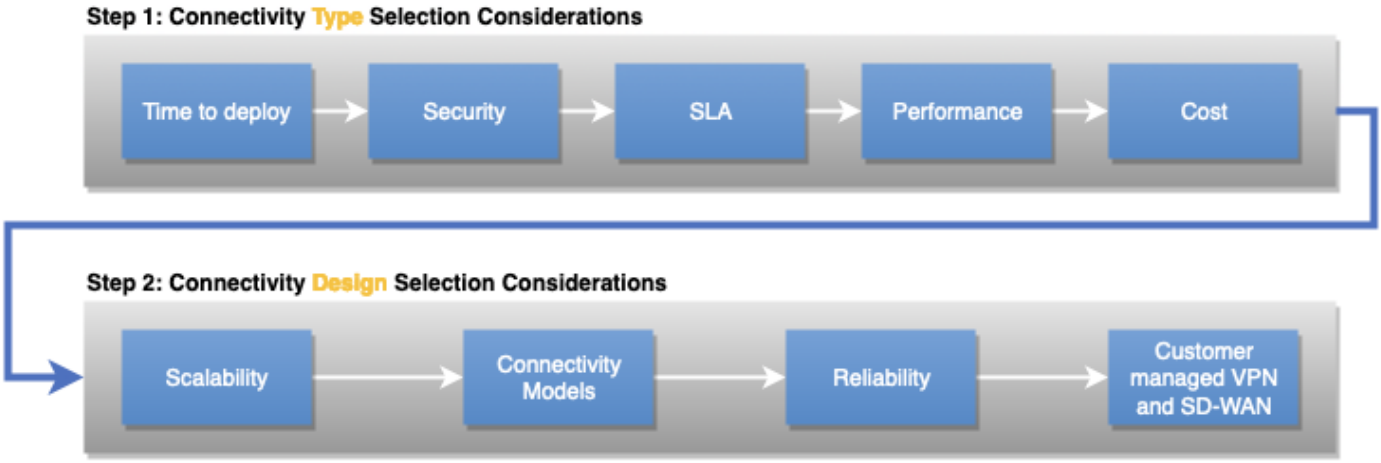

Figura 2 — Categorie di considerazione, considerazioni individuali e ordine logico tra di esse

Selezione del tipo di connettività

Questa sezione tratta le considerazioni che influiscono sul tipo di connettività selezionato per il carico di lavoro. Ciò include tempi di implementazione, sicurezza, SLA, prestazioni e costi.

Considerazioni

- È ora di implementazione
- Sicurezza
- Contratto sul livello di servizio (SLA)
- Prestazioni
- Costo

È ora di implementazione

Definizione

Il tempo di implementazione può essere un fattore importante nella scelta di un tipo di connettività adatto per un carico di lavoro. A seconda del tipo di connettività e delle ubicazioni locali, la

connettività può essere stabilita in poche ore, tuttavia potrebbero essere necessarie settimane o mesi se è necessario installare circuiti aggiuntivi. Ciò influirà sulla decisione dell'utente di utilizzare una connessione basata su Internet, una connessione privata dedicata o una connessione privata ospitata fornita come servizio gestito da un partner. AWS Direct Connect

Domande chiave

- Qual è la tempistica richiesta per l'implementazione: ore, giorni, settimane o mesi?
- Per quanto tempo sarà necessaria la connessione: si tratterà di un progetto di breve durata o di un'infrastruttura permanente?

Capacità da considerare

Se è necessaria la AWS connettività entro poche ore o giorni, è molto probabile che sia necessario utilizzare una connessione di rete esistente. Questo spesso significa stabilire una connessione VPN AWS tramite la rete Internet pubblica. Se un partner AWS DX esistente ti fornisce AWS connettività privata, una nuova connessione ospitata potrebbe essere fornita entro poche ore.

Quando hai giorni o settimane, puoi collaborare con un AWS Direct Connect partner per stabilire una connettività privata con. AWS AWS Direct Connect I partner ti aiutano a stabilire la connettività di rete tra AWS Direct Connect le sedi e il tuo data center, ufficio o ambiente di co-ubicazione. Alcuni AWS Direct Connectpartner sono autorizzati a offrire connessioni ospitate Direct Connect. Le connessioni ospitate possono spesso essere fornite più velocemente delle connessioni dedicate. AWS Direct Connect Il partner fornirà ogni connessione ospitata utilizzando l'infrastruttura esistente connessa alla AWS dorsale.

Quando hai diverse settimane o mesi, puoi valutare la possibilità di stabilire una connessione privata dedicata conAWS. I fornitori di servizi e AWS Direct Connect i partner facilitano le connessioni AWS Direct Connect dedicate. È normale che i provider di servizi installino apparecchiature di rete presso la sede del cliente per facilitare una connessione dedicata Direct Connect. A seconda del fornitore di servizi, dell'ubicazione del sito e di altri fattori fisici, l'installazione di una connessione dedicata Direct Connect può richiedere da alcune settimane a qualche mese.

Se le apparecchiature di rete sono già installate nella stessa struttura di colocation in cui si trova la AWS Direct Connect sede, è possibile stabilire rapidamente una connessione AWS Direct Connect dedicata tramite una connessione incrociata presso il sito di co-ubicazione. Dopo aver richiesto la connessione, AWS mette a disposizione una Letter of Authorization and Connecting Facility Assignment (LOA-CFA) da scaricare o invia un'e-mail con una richiesta di ulteriori informazioni. Il

LOA-CFA è l'autorizzazione alla connessione ed è richiesto dal provider di rete per AWS ordinare una connessione incrociata per conto dell'utente.

Tabella 1 — Confronto tra costi ed efficacia

	Connettività basata su Internet	Connessione dedicata DX (apparecchiature esistenti all'interno della sede DX)	Connessione dedicata DX (nuova di zecca)	Connessione ospitata DX (porta esistente con DX Partner)	Connessione ospitata DX (nuova di zecca)
Tempo di approvvigionamento	Da ore a giorni	Days	Da diverse settimane a mesi	Da ore a giorni	Da diversi giorni a settimane o mesi

> **Note**
>
> Le linee guida fornite in materia di tempi di fornitura si basano sull'osservazione del mondo reale e servono solo a titolo illustrativo. Se si prendono in considerazione l'ubicazione del sito, la vicinanza ai punti di connessione diretta e l'infrastruttura preesistente, tutto ciò influirà sui tempi di approvvigionamento. Il tuo AWS Direct Connect partner ti consiglierà l'orario preciso di approvvigionamento.

Sicurezza

Definizione

I requisiti di sicurezza influenzeranno il tipo di connettività ibrida. Queste considerazioni includono:

- Tipo di trasporto: connessione Internet o di rete privata
- Requisiti di crittografia

Domande chiave

- I requisiti e le politiche di sicurezza consentono l'uso di connessioni crittografate su Internet a cui connettersi o impongono l'uso di connessioni di rete private? AWS
- Quando si utilizzano connessioni di rete private, il livello di rete deve fornire la crittografia in transito?

Soluzioni tecniche

I requisiti e le politiche di sicurezza potrebbero consentire l'uso di Internet o richiedere l'uso di una connessione di rete privata tra la rete aziendale AWS e quella aziendale. Influiscono anche sulla decisione se la rete deve fornire la crittografia in transito o se è accettabile eseguire la crittografia a livello di applicazione.

Se riesci a sfruttare Internet, AWS Site-to-Site VPN puoi utilizzarlo per creare tunnel crittografati tra la tua rete e i tuoi Amazon VPC su InternetAWS Transit Gateway. L'estensione della soluzione SD-WAN a AWS Internet è anche un'opzione se utilizzi una connessione basata su Internet. La sezione VPN e SD-WAN gestite dal cliente più avanti in questo white paper tratta le considerazioni specifiche relative alla SD-WAN.

Se hai bisogno di una connessione di rete privata tra AWS e la tua rete aziendale, ti consigliamo di utilizzare Connessioni dedicate o Connessioni ospitate. AWS AWS Direct Connect Se è richiesta la crittografia in transito su una connessione di rete privata, è necessario stabilire una VPN tramite Direct Connect (tramite VIF pubblico o VIF di transito) oppure prendere in considerazione l'utilizzo di MacSec su una connessione dedicata da 10 Gbps o 100 Gbps.

Tabella 2 — Esempio di requisiti relativi al tipo di connettività di Automotive Corp.

	VPN da sito a sito	Direct Connect
Trasporto	Internet	Connessione di rete privata
Crittografia dei dati in transito	Sì	Richiede VPN S2S su DX, VPN S2S su un VIF di transito o MacSec su una connessione dedicata da 10 Gbps o 100 Gbps

Contratto sul livello di servizio (SLA)

Definizione

Le organizzazioni aziendali spesso richiedono che un fornitore di servizi soddisfi uno SLA per ogni servizio utilizzato dall'organizzazione. L'organizzazione a sua volta si basa sui propri servizi e può offrire ai propri consumatori uno SLA. Lo SLA è importante in quanto descrive come viene fornito e gestito il servizio e spesso include caratteristiche misurabili specifiche, come la disponibilità. Se il servizio viola lo SLA definito, un fornitore di servizi di solito offre una compensazione finanziaria specificata dal contratto. Uno SLA definisce il tipo di misura, il requisito e il periodo di misurazione. Ad esempio, fate riferimento alla definizione dell'obiettivo di uptime nell'ambito dello SLAAWS Direct Connect.

Domande chiave

- È richiesto uno SLA di connessione di connettività ibrida con crediti di servizio?
- L'intera rete ibrida deve rispettare un obiettivo di uptime?

Capacità da considerare

Tipo di connettività: la connettività Internet può essere imprevedibile. Sebbene AWS venga prestata molta attenzione alla presenza di più collegamenti con un insieme eterogeneo di ISP, l'amministrazione di Internet è semplicemente esterna al dominio amministrativo di un singolo provider AWS o al di fuori del dominio amministrativo di un singolo provider. Una volta che il traffico ha lasciato il confine della rete, un provider di servizi cloud può esercitare un numero limitato di interventi di progettazione degli itinerari e di influenza sul traffico. Detto questo, esiste uno AWS Site-to-Site VPNSLA che fornisce obiettivi di disponibilità per gli AWS Site-to-Site VPN endpoint.

AWSDirect Connect offre uno SLA formale con crediti di servizio calcolati come percentuale del totale delle tariffe AWS Direct Connect Port Hour pagate dall'utente per le connessioni applicabili che presentano indisponibilità per il ciclo di fatturazione mensile in cui lo SLA non è stato rispettato. Questo è il trasporto consigliato se è richiesto uno SLA. AWS Direct Connectelenca i requisiti minimi di configurazione specifici per ogni obiettivo di uptime, come il numero di AWS Direct Connect posizioni, connessioni e altri dettagli di configurazione. Il mancato rispetto dei requisiti significa che non è possibile offrire crediti di servizio in caso di violazione degli SLA definiti dal servizio.

È importante sottolineare che, anche se il servizio selezionato per fornire la connettività ibrida è configurato per soddisfare i requisiti SLA, il resto della rete potrebbe non fornire lo stesso livello di

SLA. La AWS responsabilità termina nel AWS Direct Connect luogo in cui si trova il AWS Direct Connect porto. Una volta AWS affidato il traffico alla rete dell'organizzazione, non è più responsabilità diAWS. Se utilizzi un provider di servizi tra AWS e la tua rete locale, la connettività è soggetta allo SLA tra te e il fornitore di servizi, se applicabile. Tieni presente che l'intera rete ibrida è valida tanto quanto la parte più debole di essa durante la progettazione della connettività ibrida.

AWS Direct Connecti partner offrono AWS Direct Connect connettività. Il partner può offrire uno SLA con crediti di servizio in base alla propria offerta di prodotti fino al punto di demarcazione con. AWS L'opzione dovrebbe essere valutata e ulteriormente ricercata direttamente con i partner APN. AWSpubblica un elenco di partner di consegna convalidati.

Progettazione logica: oltre al tipo di connettività, è necessario considerare anche altri elementi costitutivi come parte della progettazione generale. Ad esempio, AWS Transit Gatewayha un proprio SLA, così come AWSS2S VPN. Potresti utilizzare AWS Transit Gateway for scale e AWS S2S VPN per motivi di sicurezza, ma devi progettarle entrambe in modo coerente con ogni SLA per poter ottenere crediti di servizio con ogni rispettivo servizio.

Consulta i consigli sulla AWS Direct Connect resilienza e il kit di strumenti per la resilienza.

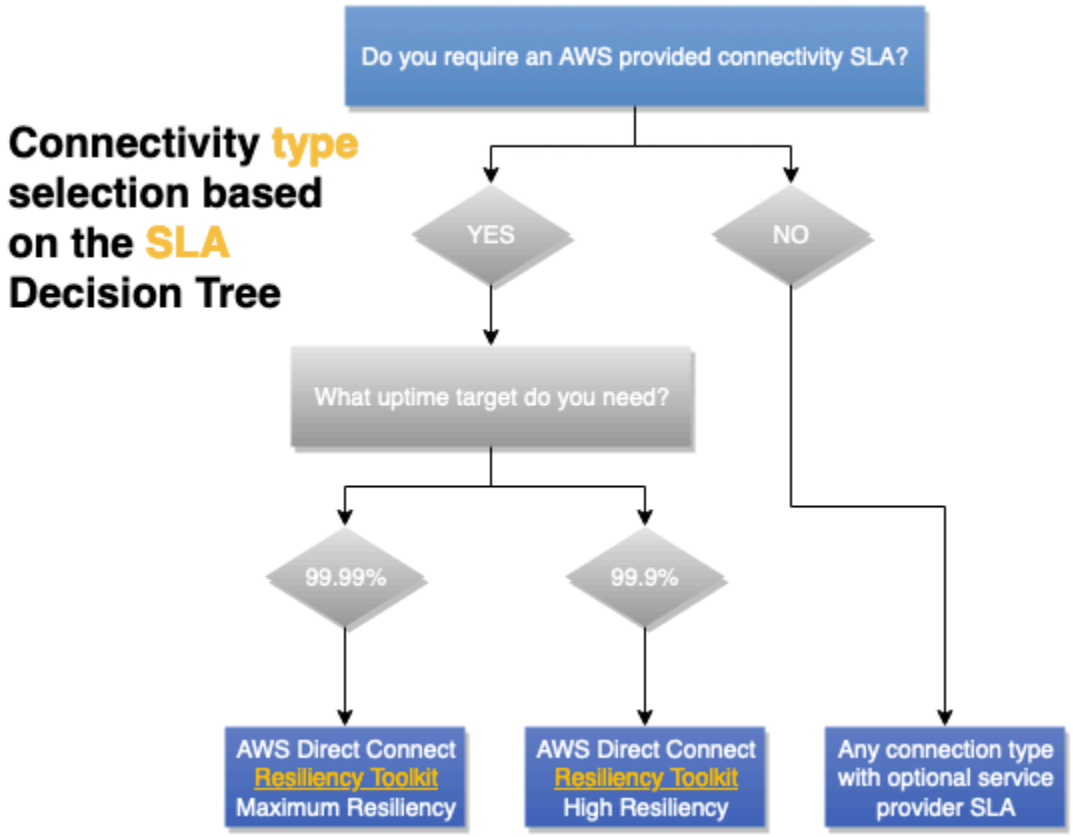

Figura 3 — Albero decisionale relativo alla considerazione dello SLA

Prestazioni

Definizione

Esistono diversi fattori che influenzano le prestazioni della rete, come la latenza, la perdita di pacchetti, il jitter e la larghezza di banda. A seconda dei requisiti dell'applicazione, l'importanza di ciascuno di questi fattori può variare.

Domande chiave

In base ai requisiti dell'applicazione, è necessario identificare e dare priorità ai fattori prestazionali della rete che influiscono sul comportamento dell'applicazione e sull'esperienza utente.

Larghezza di banda

La larghezza di banda si riferisce alla velocità di trasferimento dati di una connessione e viene generalmente misurata in bit al secondo (bps). I megabit al secondo (Mbps) e i gigabit al secondo (Gbps) sono sistemi di scalabilità comuni e sono di base 10 (1.000.000 di bit al secondo = 1 Mbps) rispetto alla base 2 (2^10) utilizzata altrove.

Nel valutare le esigenze di larghezza di banda delle applicazioni, tenete presente che i requisiti di larghezza di banda possono cambiare nel tempo. L'implementazione iniziale nel cloud, le normali operazioni, i nuovi carichi di lavoro e gli scenari di failover possono avere requisiti di larghezza di banda diversi.

Le applicazioni possono avere le proprie considerazioni sulla larghezza di banda. Alcune applicazioni potrebbero richiedere prestazioni deterministiche su una connessione a larghezza di banda elevata, mentre altre possono richiedere sia prestazioni deterministiche che larghezza di banda elevata. Un'applicazione può richiedere una configurazione speciale per utilizzare più flussi di traffico (a volte denominati stream o socket) in parallelo se raggiunge i limiti di larghezza di banda per flusso di traffico, consentendole di utilizzare una parte maggiore della larghezza di banda della connessione. Le VPN possono limitare la velocità effettiva a causa dei costi generali del tunneling, dei limiti MTU inferiori o delle limitazioni della larghezza di banda hardware.

Latenza

La latenza è il tempo necessario affinché un pacchetto passi dalla sorgente alla destinazione tramite una connessione di rete e viene generalmente misurata in millisecondi (ms), con requisiti di bassa latenza a volte espressi in microsecondi (µs). La latenza è una funzione della velocità della luce, quindi la latenza aumenta con la distanza.

I requisiti di latenza delle applicazioni possono assumere forme diverse. Un'applicazione altamente interattiva, come un desktop virtuale, può avere un obiettivo di latenza misurato dal momento in cui un utente esegue un input fino a quando l'utente vede il desktop virtuale reagire a tale input. Le applicazioni Voice over IP (VoIP) possono avere requisiti simili. Un secondo tipo di carico di lavoro da considerare sono quelli altamente transazionali, che richiedono una risposta dal server prima di poter continuare. I database o altre forme di archivi di chiave/valori possono essere fortemente influenzati dall'aumento della latenza di rete.

Jitter

Jitter misura la coerenza della latenza di rete e, come la latenza, viene generalmente misurata in millisecondi (ms).

I requisiti di jitter delle applicazioni si riscontrano in genere nelle applicazioni di streaming in tempo reale, inclusa la distribuzione di video e voce. Queste applicazioni tendono a richiedere che il flusso di dati avvenga a una velocità e un ritardo costanti, con buffer di piccole dimensioni per correggere piccole quantità di jitter.

Perdita di pacchetti

La perdita di pacchetti è la misurazione della percentuale di traffico di rete non erogata. Tutte le reti presentano a volte un certo grado di perdita di pacchetti a causa di forti picchi di traffico, riduzioni di capacità, guasti delle apparecchiature di rete e altri motivi. Pertanto, le applicazioni devono avere una certa tolleranza alla perdita di pacchetti, tuttavia, la quantità che possono tollerare può variare da un'applicazione all'altra.

Le applicazioni che utilizzano il protocollo TCP per trasportare il proprio traffico hanno la capacità di correggere la perdita di pacchetti tramite ritrasmissione. Le applicazioni che utilizzano UDP o i propri protocolli oltre all'IP devono implementare i propri mezzi per gestire la perdita di pacchetti e possono essere estremamente sensibili a tali sistemi. Un'applicazione Voice over IP può semplicemente inserire il silenzio nella parte della chiamata che ha subito la perdita di pacchetti, anziché tentare una ritrasmissione. Alcune soluzioni VPN includono meccanismi propri per il ripristino in caso di perdita di pacchetti sulla rete utilizzata per trasportare il traffico.

Capacità da considerare

Quando sono richieste latenza e velocità di trasmissione prevedibili, AWS Direct Connect è la scelta consigliata, in quanto fornisce prestazioni deterministiche. La larghezza di banda può essere selezionata in base ai requisiti di throughput. AWSse ne consiglia l'utilizzo AWS Direct Connect

quando è necessaria un'esperienza di rete più coerente rispetto a quella fornita dalle connessioni basate su Internet. I VIF privati e i Transit VIF supportano i jumbo frame, che possono ridurre il numero di pacchetti attraverso la rete e migliorare la velocità effettiva grazie alla riduzione del sovraccarico. AWS Direct Connect SiteLinkconsente di utilizzare la AWS backbone per fornire connettività tra le sedi e può essere abilitato su richiesta. La larghezza di banda utilizzata SiteLink deve essere presa in considerazione per la selezione della larghezza di banda di Direct Connect.

L'utilizzo di una VPN over AWS Direct Connect aggiunge la crittografia. Tuttavia, riduce la dimensione dell'MTU, il che potrebbe ridurre il throughput. AWSle funzionalità VPN gestite da sito a sito (S2S) sono disponibili nella documentazione. AWS Site-to-Site VPN Molte postazioni Direct Connection supportano MacSec se la crittografia della connessione è il requisito di crittografia principale. MacSec non fornisce le stesse considerazioni relative all'MTU o al potenziale throughput delle connessioni VPN da sito a sito. AWS Transit Gatewayconsente ai clienti di scalare orizzontalmente il numero di connessioni VPN e aumentare la velocità di trasmissione di conseguenza con l'Equal-cost Multi-Path Routing (ECMP). AWSLa VPN Site-to-Site gestita supporta l'utilizzo di VIF di transito Direct Connect per la connettività privata. Per ulteriori dettagli, consulta Private IP VPN con. AWS Direct Connect

Un'altra opzione è utilizzare una VPN AWS Site-to-Site gestita su Internet. Può essere un'opzione interessante grazie al basso costo ed è ampiamente disponibile. Tuttavia, tieni presente che le prestazioni su Internet sono le migliori. Gli eventi meteorologici su Internet, la congestione e l'aumento dei periodi di latenza possono essere imprevedibili. AWSoffre una soluzione con AWSAccelerated S2S VPN, che può mitigare alcuni degli aspetti negativi dell'utilizzo di un percorso Internet. Accelerated S2S VPN utilizza AWS Global Accelerator, che consente al traffico VPN di entrare nella AWS rete il prima possibile e il più vicino possibile al dispositivo gateway del cliente. Ciò ottimizza il percorso di rete utilizzando la rete AWS globale priva di congestione per indirizzare il traffico all'endpoint che fornisce le migliori prestazioni. È possibile utilizzare le connessioni VPN accelerate per evitare le interruzioni di rete che possono verificarsi quando il traffico viene indirizzato all'Internet pubblico.

Costo

Definizione

Nel cloud, il costo della connettività ibrida include il costo delle risorse fornite e dell'utilizzo. Il costo delle risorse assegnate viene misurato in unità di tempo, di solito ogni ora. L'utilizzo è per il trasferimento e l'elaborazione dei dati di solito misurato in gigabyte (GB). Gli altri costi includono il costo della connettività al punto di presenza della AWS rete. Se la rete si trova all'interno della stessa

struttura di colocation, il costo potrebbe essere inferiore a quello di una connessione incrociata. Se la rete si trova in una posizione diversa, saranno coinvolti i costi di un provider di servizi o di un partner APN Direct Connect.

Domande chiave

- Quanti dati prevedi di inviare AWS ogni mese dalla tua struttura e da Internet?
- Quanti dati prevedi di inviare AWS ogni mese alla tua struttura e a Internet?
- Con che frequenza cambieranno questi importi?
- Cosa cambia in uno scenario di fallimento?

Capacità da considerare

Se desideri eseguire carichi di lavoro che richiedono molta larghezza di bandaAWS, AWS Direct Connect puoi ridurre i costi di AWS rete in due modi. Innanzitutto, trasferendo AWS direttamente i dati da e verso, è possibile ridurre i costi della larghezza di banda pagati al provider di servizi Internet. In secondo luogo, tutti i dati trasferiti tramite la connessione dedicata vengono addebitati alla velocità di trasferimento AWS Direct Connect dati ridotta, anziché alle tariffe di trasferimento dati Internet: consulta la pagina dei prezzi di Direct Connect per i dettagli.

AWS Direct Connectconsente l'utilizzo di AWS Direct Connect SiteLink per interconnettere i siti tramite la AWS backbone: consulta il blog di SiteLink lancio per ulteriori informazioni. L'utilizzo di questa funzionalità comporta i normali costi di trasferimento dati Direct Connect, oltre a una tariffa oraria SiteLink abilitata. È possibile abilitare e disabilitare SiteLink su richiesta e può essere una buona opzione per scenari di errore che coinvolgono Internet o la connettività di rete privata.

Se utilizzi un provider di servizi di rete per la connettività tra l'ambiente locale e una posizione Direct Connect, la tua capacità e il tempo necessari per modificare gli impegni relativi alla larghezza di banda dipendono dal contratto stipulato con il fornitore di servizi.

La AWS spina dorsale è in grado di distribuire il traffico verso qualsiasi destinazione, Regione AWS tranne la Cina, da qualsiasi punto di presenza AWS della rete. Questa funzionalità presenta molti vantaggi tecnici rispetto all'utilizzo di Internet per l'accesso remotoRegioni AWS, ma ha un costo: consulta la pagina dei prezzi di EC2 Data Transfer per i dettagli. Se AWS Transit Gatewaynel percorso di traffico è presente un elemento, ciò comporta un aumento del costo di elaborazione dei dati per GB, tuttavia, se si utilizza il peering interregionale tra due gateway di transito, l'elaborazione dei dati del Transit Gateway viene fatturata una sola volta.

Il design ottimale delle applicazioni mantiene l'elaborazione dei dati entro i limiti imposti AWS e riduce al minimo i costi non necessari in uscita. L'accesso ai dati è gratuito. AWS

> **Note**
>
> Come parte della soluzione di connettività complessiva, oltre al costo della AWS connessione, è necessario considerare anche il costo della end-to-end connettività, compresi i costi del provider di servizi, le connessioni incrociate, i rack e le apparecchiature all'interno della sede DX (se necessario).

Se non siete sicuri se utilizzare Internet o una connessione privata, calcolate un punto di pareggio che AWS Direct Connect diventi meno costoso rispetto all'utilizzo di Internet. Se il volume di dati significa che AWS Direct Connect è meno costoso e hai bisogno di una connettività permanente, AWS Direct Connect è la scelta di connettività ottimale.

Se la connettività è temporanea e Internet soddisfa altri requisiti, può essere più economico utilizzare AWS S2S VPN su Internet a causa dell'elasticità di Internet. Tieni presente che ciò richiede una connettività Internet sufficiente dalla rete locale.

Se ti trovi in una struttura che dispone di AWS Direct Connect (l'elenco è disponibile sul sito Web di Direct Connect), puoi stabilire una connessione incrociata aAWS. Ciò significa utilizzare connessioni dedicate a 1,10 o 100 Gbps. AWS Direct Connecti partner offrono più opzioni di larghezza di banda e capacità inferiori, il che può ottimizzare i costi di connettività. Ad esempio, puoi iniziare con una connessione ospitata da 50 Mbps anziché da una connessione dedicata da 1 Gbps.

ConAWS Transit Gateway, puoi condividere le tue connessioni VPN e Direct Connect con molti VPC. Oltre a essere addebitato in base al numero di connessioni effettuate AWS Transit Gateway all'ora e alla quantità di traffico in transitoAWS Transit Gateway, ciò semplifica la gestione e riduce il numero di connessioni VPN e VIF richieste. I vantaggi e i risparmi sui costi derivanti da un minore sovraccarico operativo possono facilmente superare i costi aggiuntivi dell'elaborazione dei dati. Facoltativamente, puoi prendere in considerazione un progetto che AWS Transit Gateway si trovi nel percorso di traffico verso la maggior parte dei VPC, ma non tutti. Questo approccio consente di evitare i costi di elaborazione dei AWS Transit Gateway dati nei casi d'uso in cui è necessario trasferire grandi quantità di dati. AWS Consultate la sezione Modelli di connettività per ulteriori dettagli su questo design. Un altro approccio consiste nell'utilizzare AWS Direct Connect come percorso principale la VPN AWS S2S su Internet come percorso di backup/failover. Sebbene tecnicamente fattibile e molto conveniente, questa soluzione presenta degli svantaggi tecnici

(discussi nella sezione Affidabilità di questo white paper) e può essere più difficile da gestire. AWSnon lo consiglia per carichi di lavoro altamente critici o critici.

L'approccio finale è una VPN o SD-WAN gestita dal cliente e distribuita nelle istanze di Amazon EC2. Questo può essere più economico su larga scala se ci sono da decine a centinaia di siti rispetto alla VPN S2S. AWS Tuttavia, è necessario prendere in considerazione i costi generali di gestione, i costi di licenza e il costo delle risorse EC2 per ogni appliance virtuale.

Matrice decisionale

Tabella 3 — Esempi di input per la progettazione della connettività automobilistica di Example Corp.

Categoria	VPN o SD-WAN gestita dal cliente	AWSVPN S2S	AWSVPN S2S accelerata	AWS Direct ConnectConnessione ospitata	AWS Direct ConnectConnessione dedicata
Richiede una connessione a Internet	Sì	Sì	Sì	No	No
Costo delle risorse fornite	Licenze software e istanze EC2	AWSVPN S2S	AWSVPN S2S e Global Accelerator AWS	Parte del costo della porta in termini di capacità applicabile	Costo della porta dedicata
Costo di trasferimento dei dati	Tariffa Internet	Tariffa Internet o tariffa Direct Connect	Internet con trasferimento dati premium	Tariffa Direct Connect	Tariffa Direct Connect
Gateway di transito	Facoltativo	Facoltativo	Obbligatorio	Facoltativo	Facoltativo
AWSCosto di elaborazione dei dati	N/D	Solo con AWS Transit Gateway	Sì	Solo con AWS Transit Gateway	Solo con AWS Transit Gateway

Categoria	VPN o SD-WAN gestita dal cliente	AWSVPN S2S	AWSVPN S2S accelerata	AWS Direct ConnectConnessione ospitata	AWS Direct ConnectConnessione dedicata
Può essere riutilizzatoAWS Direct Connect?	Sì	Sì	No	N/D	N/D

Selezione del design della connettività

Questa sezione del white paper illustra le considerazioni che influiscono sulla scelta del design della connettività. La progettazione della connettività include gli aspetti logici e le modalità di progettazione e ottimizzazione dell'affidabilità della connettività ibrida.

Verranno trattate le seguenti considerazioni: scalabilità, modelli di connettività, affidabilità, gestione dal cliente VPN e SD-. WAN

Considerazioni

- Scalabilità
- Modelli di connettività
- Affidabilità
- Gestito dal cliente VPN e SD- WAN

Scalabilità

Definizione

La scalabilità si riferisce alla capacità della soluzione di connettività di crescere ed evolversi nel tempo al variare delle esigenze.

Quando si progetta una soluzione, è necessario considerare le dimensioni attuali e la crescita prevista. Questa crescita può essere una crescita organica o può essere correlata a una rapida espansione, ad esempio negli scenari di fusione e acquisizione.

Nota: a seconda dell'architettura della soluzione mirata, potrebbe non essere necessario prendere in considerazione tutti gli elementi precedenti. Tuttavia, possono fungere da elementi fondamentali per identificare i requisiti di scalabilità delle soluzioni di rete ibride più comuni. Questo white paper si concentra sulla selezione e sulla progettazione della connettività ibrida. Si consiglia di considerare anche la scala della connettività ibrida rispetto all'VPCarchitettura di rete. Per ulteriori informazioni, consulta il white paper Creazione di un'infrastruttura VPC AWS multirete scalabile e sicura.

Domande chiave

- Qual è il numero attuale e previsto di VPCs cui è necessaria la connettività al sito o ai siti locali?
- Sono VPCs distribuiti in una Regione AWS o più regioni?
- A quanti siti locali è necessario connettersi? AWS
- Quanti dispositivi gateway per i clienti (in genere router o firewall) avete per sito a cui dovete connettervi? AWS
- Quanti percorsi dovrebbero essere pubblicizzati su Amazon VPCs e qual è il numero di percorsi previsti che verranno ricevuti da Amazon AWS ?
- È necessario aumentare la larghezza di banda AWS nel tempo?

Capacità da considerare

La scalabilità è un fattore importante nella progettazione della connettività ibrida. A quel punto, la sezione successiva incorporerà la scala come parte della progettazione del modello di connettività mirato.

Di seguito sono riportate le best practice consigliate per ridurre al minimo la complessità di scala della progettazione della connettività di rete ibrida:

- È necessario utilizzare il riepilogo dei percorsi per ridurre il numero di percorsi pubblicizzati e ricevuti da. AWS Pertanto, lo schema di indirizzamento IP deve essere progettato per massimizzare l'uso del riepilogo delle rotte. L'ingegneria del traffico è una considerazione generale fondamentale. Per ulteriori informazioni sull'ingegneria del traffico, consulta la sottosezione Ingegneria del traffico nella sezione Affidabilità.
- Riduci al minimo il numero di sessioni di BGP peering utilizzando DXGW with VGW or AWS Transit Gateway, laddove una singola BGP sessione può fornire connettività a più sessioni. VPCs
- Prendi in considerazione il cloud WAN quando è necessario connettere più Regioni AWS siti locali.

Modelli di connettività

Definizione

Il modello di connettività si riferisce al modello di comunicazione tra le reti locali e le risorse cloud in. AWS Puoi distribuire risorse cloud all'interno di un Amazon VPC all'interno di una Regione AWS o più VPCs regioni, nonché AWS servizi che hanno un endpoint pubblico in una o più regioni Regioni AWS, come Amazon S3 e DynamoDB.

Domande chiave

- È necessaria l'VPCintercomunicazione all'interno di una regione e tra le regioni?
- È necessario accedere agli endpoint AWS pubblici direttamente dall'ambiente locale?
- È necessario accedere ai AWS servizi utilizzando gli VPC endpoint dall'ambiente locale?

Funzionalità da considerare

Di seguito sono riportati alcuni degli scenari di modelli di connettività più comuni. Ogni modello di connettività copre requisiti, attributi e considerazioni.

Nota: come evidenziato in precedenza, questo white paper è incentrato sulla connettività ibrida tra reti locali e. AWS Per ulteriori dettagli sulla progettazione dell'interconnessioneVPCs, consulta il white paper Costruire un'infrastruttura multirete scalabile e sicura. VPC AWS

Modelli

- AWS Accelerata: singola Site-to-Site VPN AWS Transit GatewayRegione AWS
- AWS DX: DXGW conVGW, Single Region
- AWS DX: DXGW con multiregioni VGW e peering pubblico AWS
- AWS DX: DXGW con multiregioni AWS Transit Gateway e peering pubblico AWS
- AWS DX: DXGW con AWS Transit Gateway più regioni (più di 3)

AWS Accelerata: singola Site-to-Site VPN AWS Transit GatewayRegione AWS

Questo modello è composto da:

- Singola Regione AWS.

- AWS Site-to-SiteVPNConnessione gestita con AWS Transit Gateway.
- Accelerata VPN abilitata.

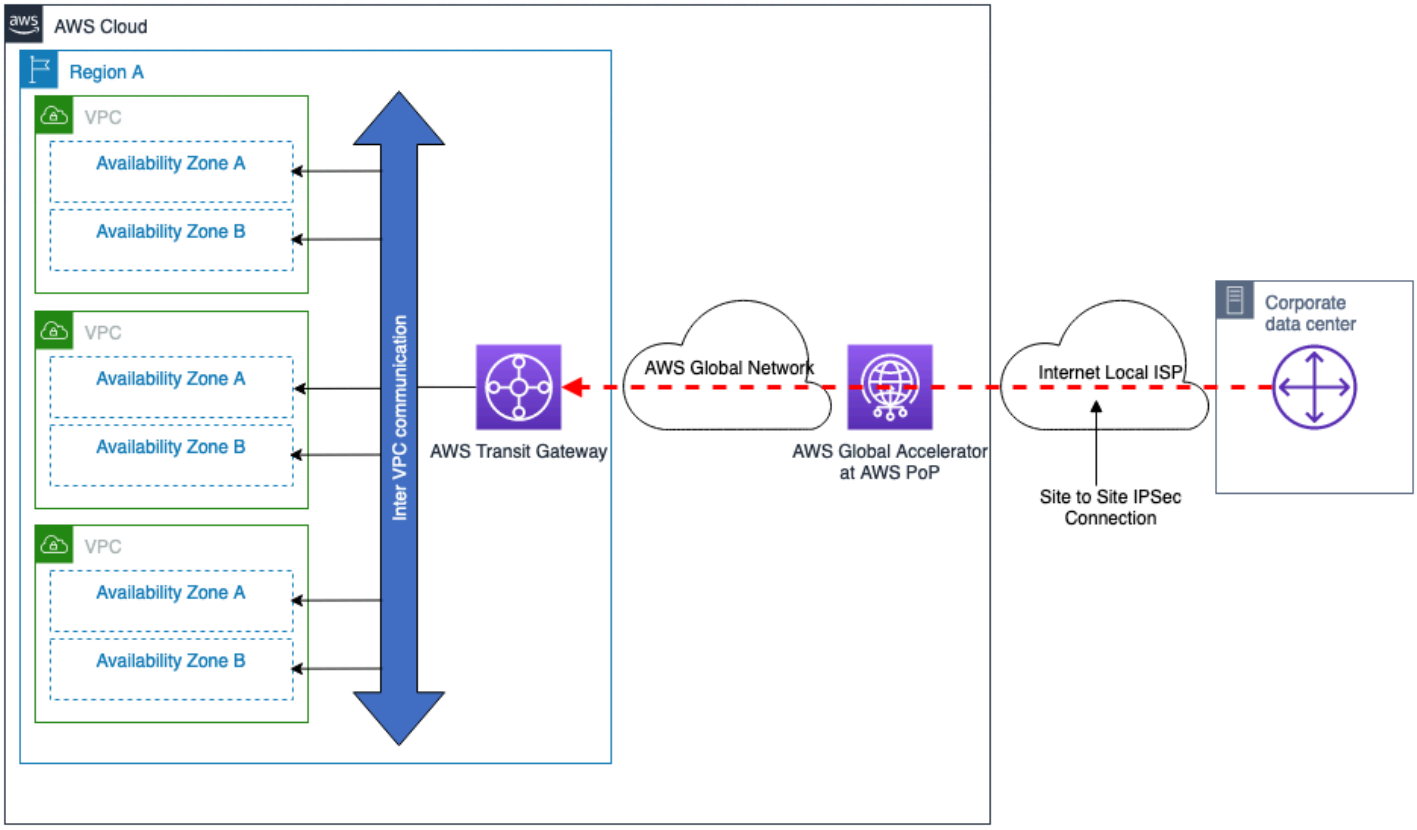

Figura 4 — AWS Gestito VPN — AWS Transit Gateway, Singolo Regione AWS

Attributi del modello di connettività:

- Offri la possibilità di stabilire VPN connessioni ottimizzate sulla rete Internet pubblica utilizzando Site-to-SiteVPNconnessioni AWS accelerate.
- Offri la possibilità di ottenere una maggiore larghezza di banda di VPN connessione configurando più VPN tunnel con. ECMP
- Può essere utilizzato per la connessione da più siti remoti.
- Offre un failover automatizzato con routing dinamico ()BGP.
- Con AWS Transit Gateway connected toVPCs, tutte le persone connesse VPCs possono utilizzare le stesse VPN connessioni. Puoi anche controllare il modello di comunicazione desiderato tra i seguentiVPCs, per maggiori informazioni consulta How Transit Gateway Work.

- Offre opzioni di progettazione flessibili per integrare dispositivi di sicurezza di terze parti e dispositivi WAN virtuali SD con AWS Transit Gateway. Vedi Sicurezza di rete centralizzata per il VPC-to-VPC traffico e in locale. VPC

Considerazioni sulla scalabilità:

- Fino a 50 Gbps di larghezza di banda con più IPsec tunnel e ECMP configurati (ogni flusso di traffico sarà limitato alla larghezza di banda massima per tunnel). VPN
- È VPCs possibile collegarne migliaia per. AWS Transit Gateway
- Fai riferimento alle Site-to-Site VPNquote per altri limiti di scala, come il numero di rotte.

Altre considerazioni:

- I costi di AWS Transit Gateway elaborazione aggiuntivi per il trasferimento dei dati tra il data center locale e. AWS
- Non è VPC possibile fare riferimento ai gruppi di sicurezza di un telecomando AWS Transit Gateway , ma ciò è supportato dal VPC peering.

AWS DX: DXGW conVGW, Single Region

Questo modello è composto da:

- Singola Regione AWS.
- Doppie AWS Direct Connect connessioni a postazioni DX indipendenti.
- AWS DXGWdirettamente collegato all'VPCsutilizzoVGW.
- Utilizzo opzionale di AWS Transit Gateway per l'VPCintercomunicazione.

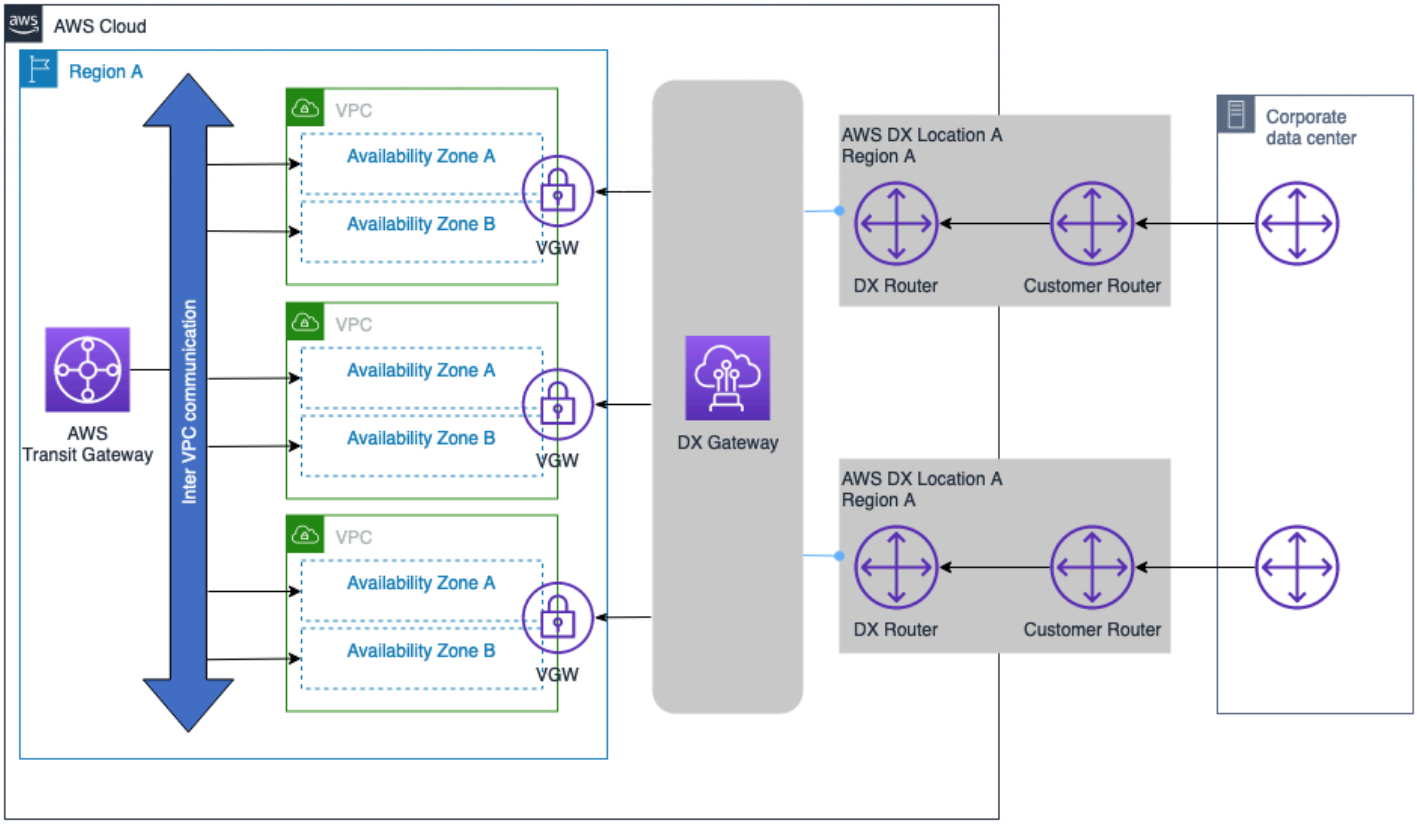

Figura 5 — AWS DX — DXGW con, Single VGW Regione AWS

Attributi del modello di connettività:

- Offre la possibilità di connettersi a VPCs connessioni DX in altre regioni in futuro.
- Offre un failover automatizzato con routing dinamico (). BGP
- Con AWS Transit Gateway puoi controllare il modello di comunicazione desiderato tra i. VPCs Per ulteriori informazioni, consulta Come funzionano i gateway di transito.

Considerazioni sulla scalabilità:

Fai riferimento alle AWS Direct Connect quote per ulteriori informazioni su altri limiti di scala, come il numero di prefissi supportati, il numero VIFs per tipo di connessione DX (dedicata, ospitata). Alcune considerazioni chiave:

- La BGP sessione privata VIF può pubblicizzare fino a 100 percorsi ciascuno per IPv4 e. IPv6

- VPCsÈ possibile collegarne fino a 20 per DXGW singola BGP sessione. Se VPCs sono necessari più di 20, è DXGWs possibile aggiungerne altri per facilitare la connettività su larga scala oppure prendere in considerazione l'utilizzo dell'integrazione Transit Gateway.
- Se necessario AWS Direct Connect, è possibile aggiungere altri messaggi.

Altre considerazioni:

- Non comporta i AWS Transit Gateway relativi costi di elaborazione per il trasferimento di dati tra reti locali AWS e tra reti locali.
- Non è VPC possibile fare riferimento ai gruppi di sicurezza di un telecomando AWS Transit Gateway (è necessario il peering). VPC
- VPCil peering può essere utilizzato anziché AWS Transit Gateway per facilitare la comunicazione tra iVPCs, tuttavia ciò aggiunge complessità operativa per creare e gestire il VPC point-to-point peering di grandi numeri su larga scala.
- Se non è richiesta l'VPCintercomunicazione, in questo modello di connettività non è necessario AWS Transit Gateway né il VPC peering né il peering.

AWS DX: DXGW con multiregioni VGW e peering pubblico AWS

Questo modello è composto da:

- Più data center locali con doppie connessioni a AWS.
- Doppie AWS Direct Connect connessioni a postazioni DX indipendenti.
- AWS DXGWcollegato direttamente a più di 10 VPCs utilizziVGW, fino a 20 VPCs utilizziVGW.
- Utilizzo opzionale di AWS Transit Gateway per la comunicazione interregionale VPC e interregionale.

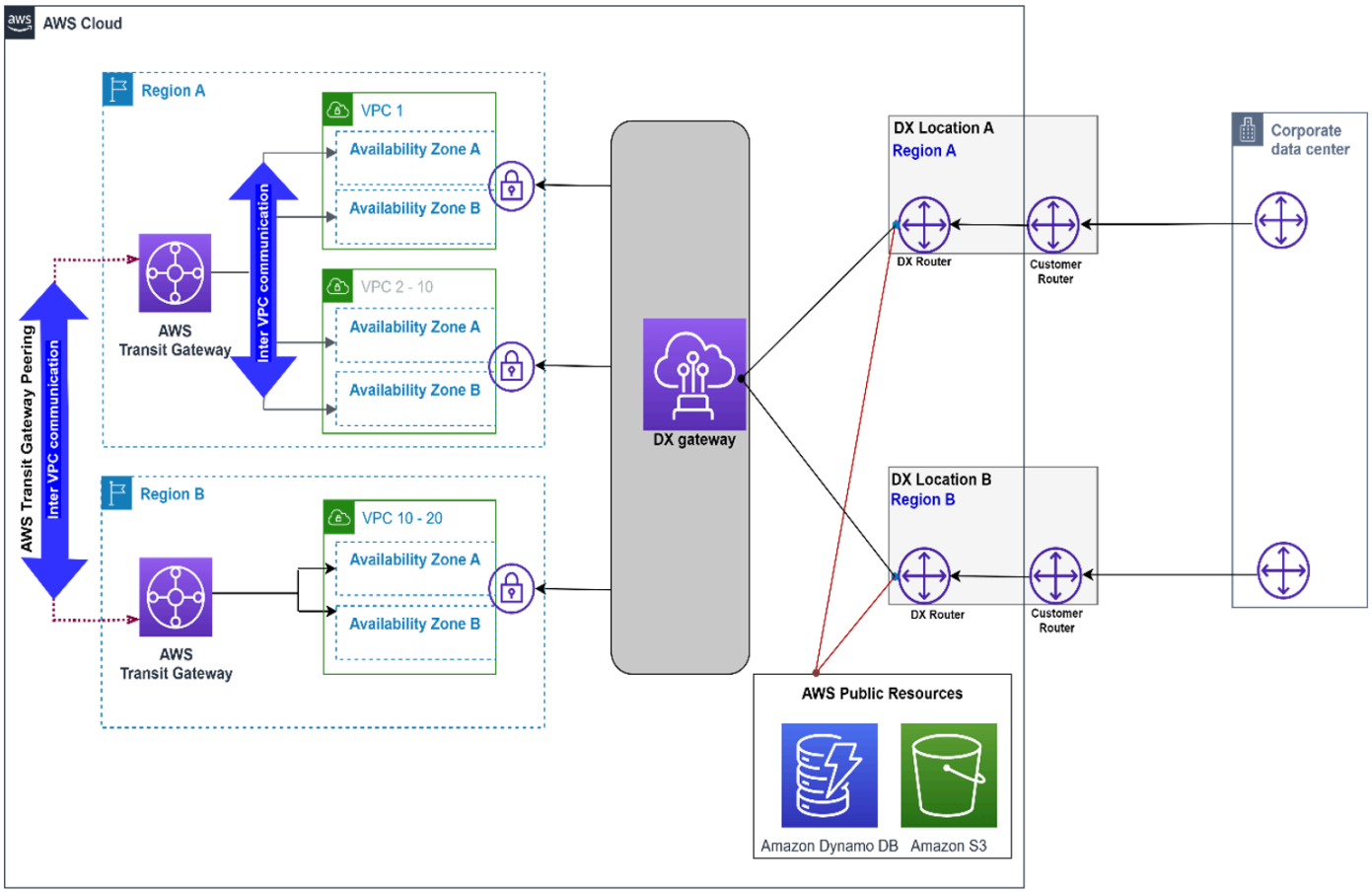

Figura 6 — AWS DX: DXGW con più regioni VGW e pubblico VIF

Attributi del modello di connettività:

- AWS DXGWcollegato direttamente a più di 10 VPCs VGW utilizzandone fino a 20 VPCsVGW.
- AWS DX public VIF viene utilizzato per accedere a servizi AWS pubblici, come Amazon S3, direttamente tramite AWS le connessioni DX.
- Offri la possibilità di connetterti a VPCs connessioni DX in altre regioni in futuro.
- VPCComunicazione interregionale VPC e interregionale facilitata dal peering del Transit AWS Transit Gateway Gateway.

Considerazioni sulla scala:

Fai riferimento alle AWS Direct Connect quote per ulteriori informazioni su altri limiti di scala, come il numero di prefissi supportati, il numero VIFs per tipo di connessione DX (dedicata, ospitata). Alcune considerazioni chiave:

- La BGP sessione privata VIF può pubblicizzare fino a 100 percorsi ciascuno per IPv4 e. IPv6
- VPCsÈ possibile connetterne fino a 20 per DXGW ogni BGP sessione privataVIF, fino a 30 VIFs per sessione privata. DXGW
- Se lo desideri, puoi aggiungere altri AWS Direct Connect messaggi.

Altre considerazioni:

- Non comporta i AWS Transit Gateway relativi costi di elaborazione per il trasferimento di dati tra reti locali AWS e tra reti locali.
- I gruppi di sicurezza di un telecomando VPC non possono essere referenziati da AWS Transit Gateway (è necessario il peering). VPC
- VPCil peering può essere utilizzato anziché AWS Transit Gateway per facilitare la comunicazione tra iVPCs, tuttavia ciò aggiungerà complessità operativa per creare e gestire il VPC point-to-point peering di grandi numeri su larga scala.
- Se non è richiesta l'VPCintercomunicazione, in questo modello di connettività non è necessario AWS Transit Gateway né il VPC peering né il peering.

AWS DX: DXGW con multiregioni AWS Transit Gateway e peering pubblico AWS

Questo modello è composto da:

- Multiplo Regioni AWS.
- Doppie AWS Direct Connect connessioni a postazioni DX indipendenti.
- Singolo data center locale con doppie connessioni a. AWS
- AWS DXGWcon AWS Transit Gateway.
- Scala elevata VPCs per regione.

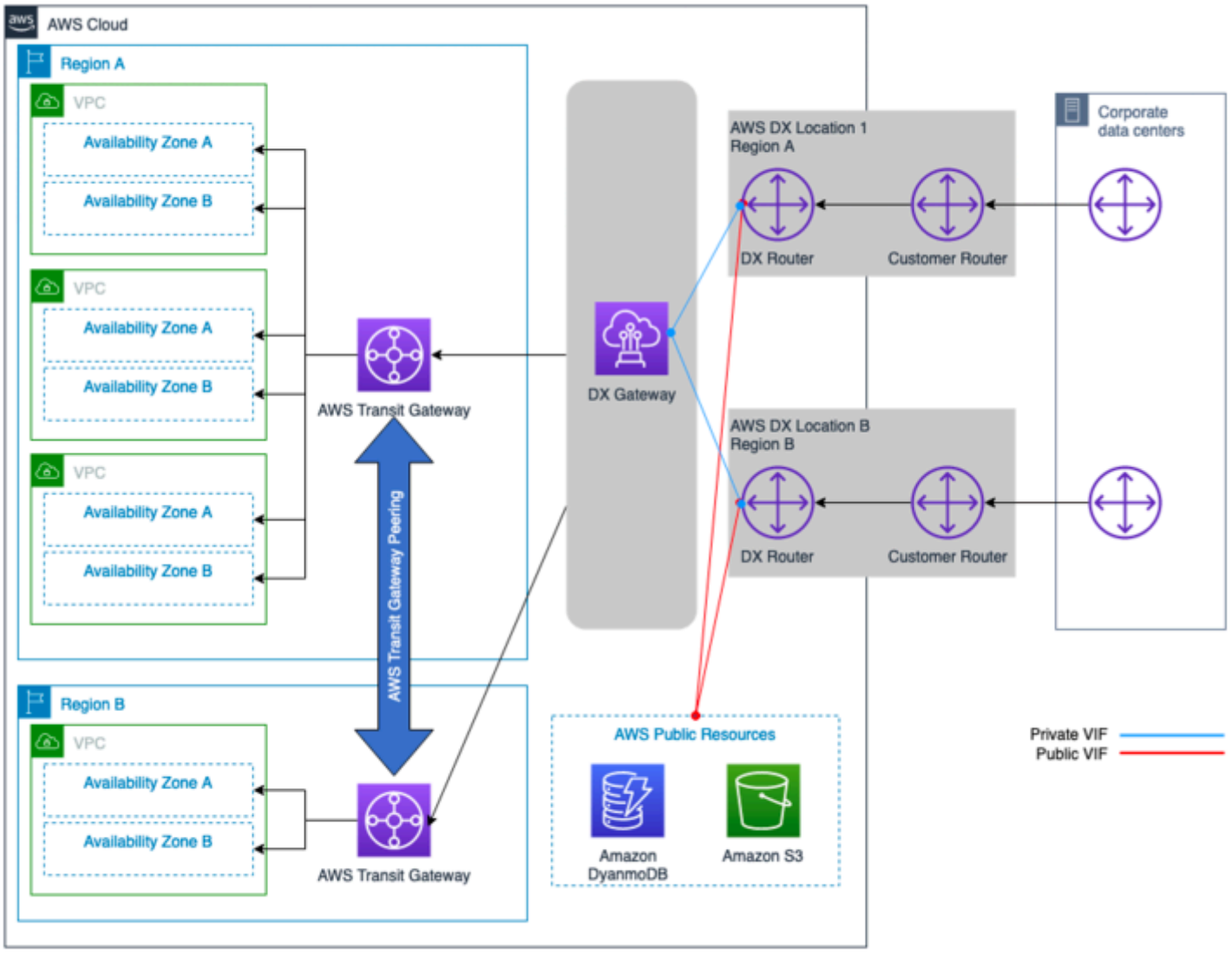

Figura 7 — AWS DX: DXGW con AWS Transit Gateway, multiregioni e pubblico AWS VIF

Attributi del modello di connettività:

- AWS DX public VIF viene utilizzato per accedere a risorse AWS pubbliche come S3 direttamente tramite le connessioni AWS DX.
- Offri la possibilità di connetterti VPCs e/o connessioni DX in altre regioni in futuro.
- Con AWS Transit Gateway connected toVPCs, è possibile ottenere una connettività mesh totale o parziale tra. VPCs
- VPCComunicazione interregionale VPC e interregionale facilitata dal peering. AWS Transit Gateway

- Offre opzioni di progettazione flessibili con cui integrare dispositivi di sicurezza e SDWAN virtuali di terze parti. AWS Transit Gateway Vedi: Sicurezza di rete centralizzata per il VPC-to-VPC traffico e in locale. VPC

Considerazioni sulla scalabilità:

- Il numero di rotte da e verso AWS Transit Gateway è limitato al numero massimo supportato di rotte su un transito VIF (i numeri in entrata e in uscita variano). Fai riferimento alle AWS Direct Connect quote per ulteriori informazioni sui limiti di scala e sul numero di rotte supportato e. VIFs
- Scalabilità fino a AWS Transit Gateway migliaia VPCs per BGP sessione singola.
- Transito singolo VIF per AWS DX.
- Se necessario, è possibile aggiungere ulteriori connessioni AWS DX.

Altre considerazioni:

- Comporta costi di AWS Transit Gateway elaborazione aggiuntivi per il trasferimento dei dati tra AWS e il sito locale.
- I gruppi di sicurezza di un telecomando VPC non possono essere referenziati da AWS Transit Gateway (è necessario VPC il peering).
- VPCil peering può essere utilizzato anziché AWS Transit Gateway per facilitare la comunicazione tra iVPCs, tuttavia ciò aggiungerà complessità operativa per creare e gestire il VPC point-to-point peering di grandi numeri su larga scala.

AWS DX: DXGW con AWS Transit Gateway più regioni (più di 3)

Questo modello è composto da:

- Multiplo Regioni AWS (più di 3).
- Due data center locali.
- Doppie AWS Direct Connect connessioni verso sedi DX indipendenti per regione.
- AWS DXGWcon AWS Transit Gateway.
- Scala elevata VPCs per regione.
- Maglia completa di scrutinio tra AWS Transit Gateway s.

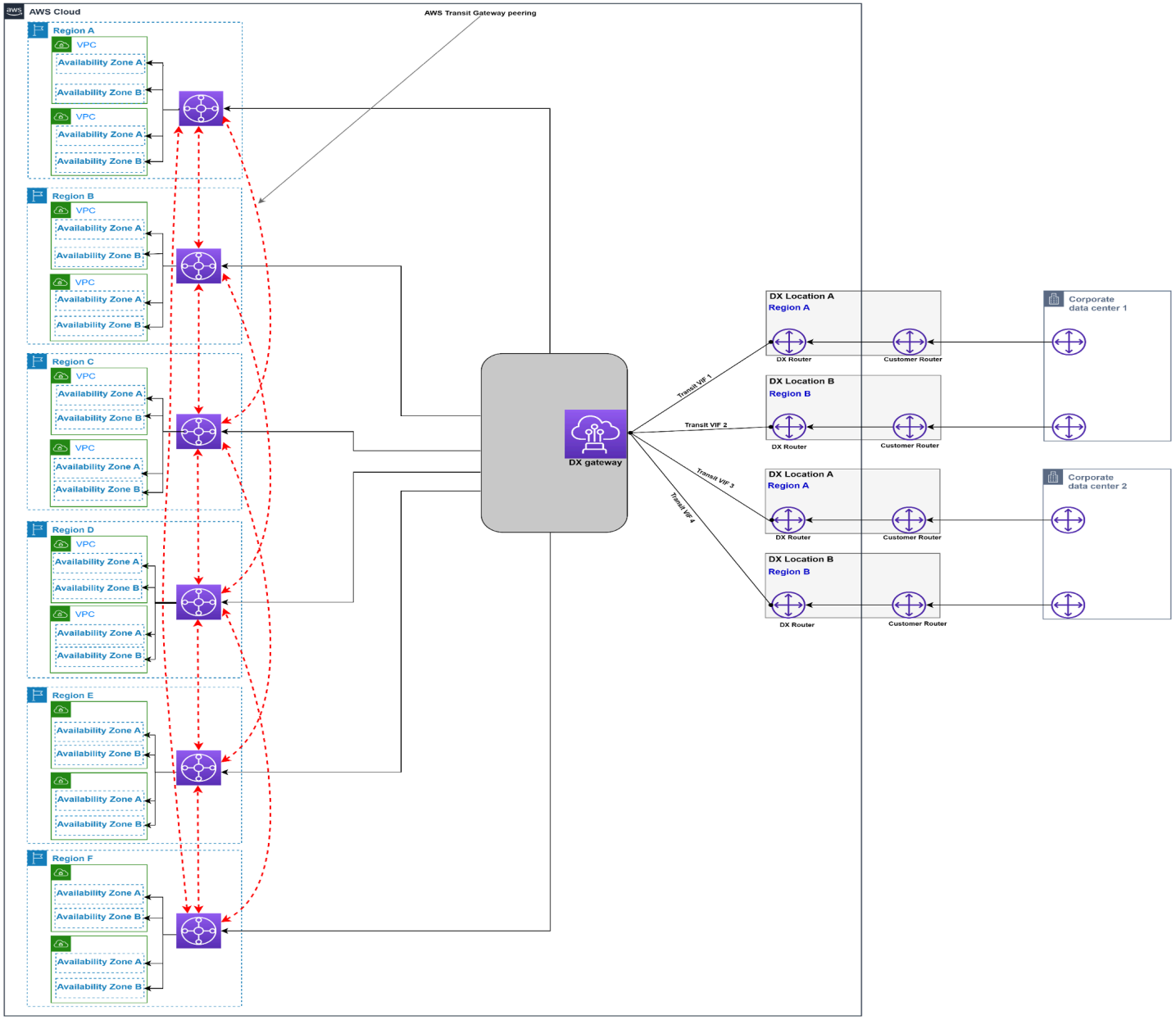

Figura 8 — AWS DX — DXGW con AWS Transit Gateway, più regioni (più di tre)

Attributi del modello di connettività:

- Sovraccarico operativo più basso.
- AWS DX public VIF viene utilizzato per accedere a risorse AWS pubbliche, come S3, direttamente tramite le AWS connessioni DX.
- Offri la possibilità di connetterti a VPCs connessioni DX in altre regioni in futuro.

- Con AWS Transit Gateway connected toVPCs, è possibile ottenere una connettività mesh completa o parziale tra. VPCs
- La VPC comunicazione interregionale è facilitata dal peering. AWS Transit Gateway
- Offre opzioni di progettazione flessibili con cui integrare dispositivi di sicurezza e SDWAN virtuali di terze parti. AWS Transit Gateway Vedi: Sicurezza di rete centralizzata per il VPC-to-VPC traffico e in locale. VPC

Considerazioni sulla scalabilità:

- Il numero di rotte da e verso AWS Transit Gateway è limitato al numero massimo supportato di rotte su un transito VIF (i numeri in entrata e in uscita variano). Fai riferimento alle AWS Direct Connect quote per ulteriori informazioni sui limiti di scala. Se necessario, prendi in considerazione la possibilità di riepilogare i percorsi per ridurne il numero.
- Scalabilità fino a AWS Transit Gateway migliaia VPCs per BGP sessione per sessione DXGW (supponendo che le prestazioni fornite dalle connessioni AWS DX fornite siano sufficienti).
- È possibile connettere fino a sei AWS Transit Gateway secondi per volta. DXGW
- Se è necessario collegare più di tre regioni utilizzando AWS Transit Gateway, ne DXGWs sono necessarie altre.
- Transito singolo VIF per AWS DX.
- Se necessario, è possibile aggiungere ulteriori connessioni AWS DX.

Altre considerazioni:

- Comporta costi di AWS Transit Gateway elaborazione aggiuntivi per il trasferimento dei dati tra il sito locale e. AWS
- I gruppi di sicurezza di un telecomando VPC non possono essere referenziati da AWS Transit Gateway (è necessario VPC il peering).
- VPCil peering può essere utilizzato invece che AWS Transit Gateway per facilitare la comunicazione tra iVPCs, tuttavia ciò aggiungerà complessità operativa per creare e gestire il VPC point-to-point peering di grandi numeri su larga scala.

Il seguente albero decisionale copre le considerazioni sulla scalabilità e sul modello di comunicazione:

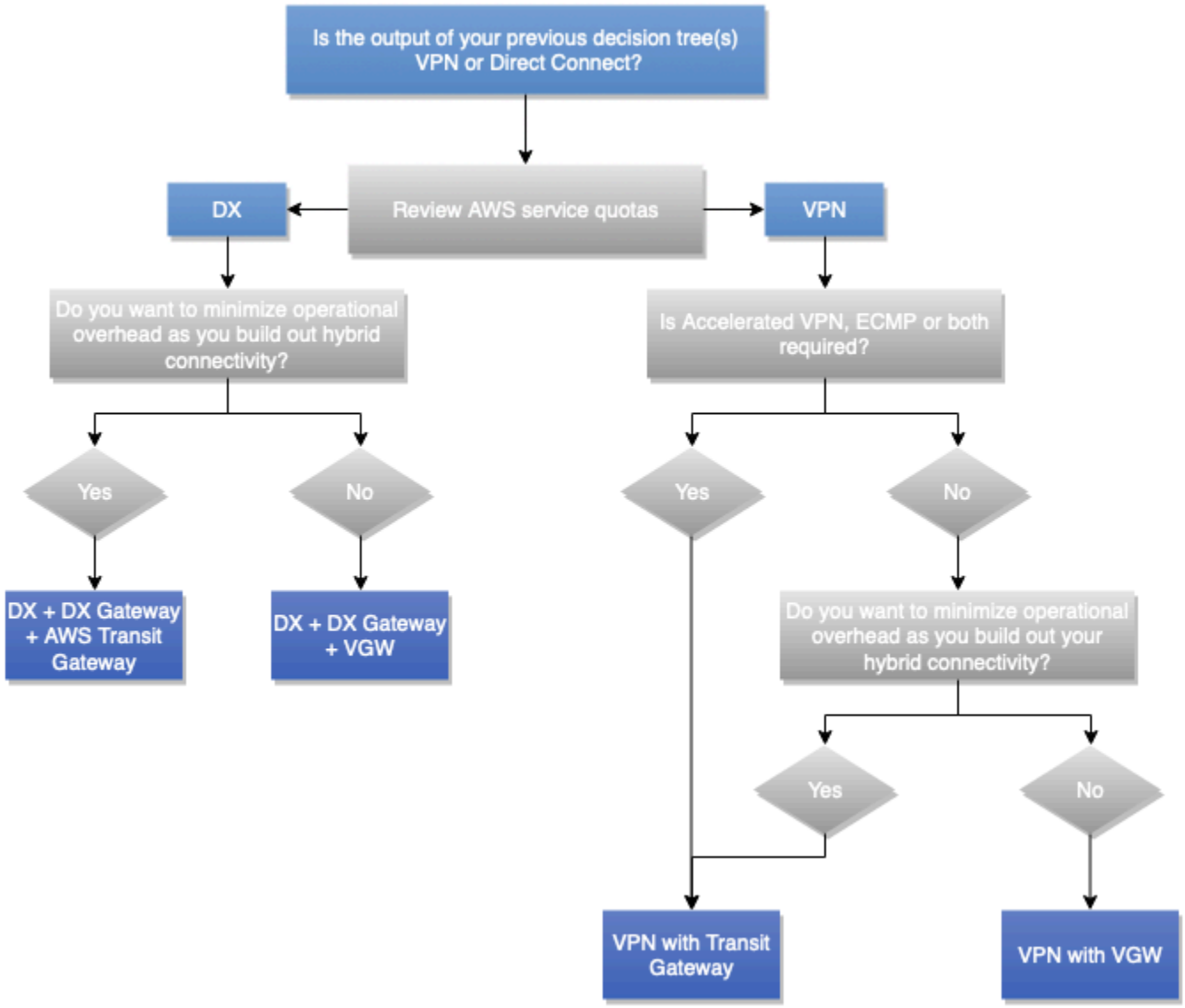

Figura 9 — Albero decisionale del modello di scalabilità e comunicazione

> **Note**
>
> Se il tipo di connessione selezionato èVPN, in genere, tenuto conto delle prestazioni, è necessario decidere se il punto di VPN terminazione sia una connessione AWS VGW AWS Transit Gateway AWS VPN S2S. Se non l'hai ancora fatto, puoi prendere in considerazione il modello di comunicazione richiesto tra i e il numero di connessioni necessarie VPC per il VPN collegamento alle connessioni per aiutarti a prendere la decisione. VPC

Affidabilità

Definizione

L'affidabilità si riferisce alla capacità di un servizio o di un sistema di svolgere la funzione prevista quando richiesto. L'affidabilità di un sistema può essere misurata in base al livello della sua qualità operativa entro un determinato periodo di tempo. Paragonalo alla resilienza, che si riferisce alla capacità di un sistema di riprendersi da interruzioni dell'infrastruttura o del servizio, in modo dinamico e affidabile.

Per maggiori dettagli su come la disponibilità e la resilienza vengono utilizzate per misurare l'affidabilità, consulta il Reliability Pillar del Well-Architected AWS Framework.

Domande chiave

Disponibilità

La disponibilità è la percentuale di tempo per cui un carico di lavoro è disponibile per l'uso. Gli obiettivi comuni includono il 99% (3,65 giorni di inattività consentiti all'anno), il 99,9% (8,77 ore) e il 99,99% (52,6 minuti), con un'abbreviazione del numero di nove nella percentuale («due nove» per il 99%, «tre nove» per il 99,9% e così via). La disponibilità della soluzione di rete tra AWS e il data center locale può essere diversa dalla disponibilità complessiva della soluzione o dell'applicazione.

Le domande chiave sulla disponibilità di una soluzione di rete includono:

- Le mie AWS risorse possono continuare a funzionare se non riescono a comunicare con le mie risorse locali? Viceversa?
- Devo considerare i tempi di inattività programmati per la manutenzione pianificata inclusi o esclusi dalla metrica di disponibilità?
- Come posso misurare la disponibilità del livello di rete, indipendentemente dallo stato generale delle applicazioni?

La sezione Availability del Well-Architected Framework Reliability Pillar contiene suggerimenti e formule per la disponibilità dei calcoli.

Resilienza

La resilienza è la capacità di un carico di lavoro di ripristinarsi a seguito di interruzioni dell'infrastruttura o del servizio, acquisire in modo dinamico le risorse di calcolo per soddisfare la

domanda e mitigare le interruzioni, quali configurazioni errate o problemi di rete transitori. Se un componente di rete ridondante (collegamento, dispositivi di rete e così via) non dispone di una disponibilità sufficiente per fornire da solo la funzione prevista, ha una bassa resilienza ai guasti. La conseguenza è un'esperienza utente scadente e degradata.

Le domande chiave per la resilienza di una soluzione di rete includono:

- Quanti guasti simultanei e discreti devo consentire?
- Come posso ridurre i singoli punti di errore sia con le soluzioni di connettività che con la mia rete interna?
- Qual è la mia vulnerabilità agli eventi Distributed Denial of Service (DDoS)?

Soluzione tecnica

Innanzitutto, è importante notare che non tutte le soluzioni di connettività di rete ibrida richiedono un elevato livello di affidabilità e che livelli crescenti di affidabilità comportano un corrispondente aumento dei costi. In alcuni scenari, un sito primario può richiedere connessioni affidabili (ridondanti e resilienti) poiché i tempi di inattività hanno un impatto maggiore sull'attività, mentre i siti regionali potrebbero non richiedere lo stesso livello di affidabilità a causa del minore impatto sull'attività in caso di guasto. Si consiglia di fare riferimento alle raccomandazioni sulla AWS Direct Connect resilienza in quanto spiegano le AWS migliori pratiche per garantire un'elevata resilienza in fase di progettazione. AWS Direct Connect

Per ottenere una soluzione di connettività di rete ibrida affidabile nel contesto della resilienza, la progettazione deve prendere in considerazione i seguenti aspetti:

- Ridondanza: mira a eliminare ogni singolo punto di errore nel percorso di connettività di rete ibrida, inclusi, a titolo esemplificativo, le connessioni di rete, i dispositivi di rete periferici, la ridondanza tra le zone di disponibilità e le posizioni DX Regioni AWS, le fonti di alimentazione dei dispositivi, i percorsi in fibra e i sistemi operativi. Per lo scopo e l'ambito di questo white paper, la ridondanza si concentra sulle connessioni di rete, sui dispositivi periferici (ad esempio, i dispositivi gateway del cliente), sulla posizione AWS DX e Regioni AWS (per le architetture multiregionali).
- Componenti di failover affidabili: in alcuni scenari, un sistema potrebbe funzionare, ma non svolgere le sue funzioni al livello richiesto. Una situazione di questo tipo è comune nel caso di un singolo evento di guasto, in cui si scopre che i componenti ridondanti pianificati funzionavano in modo non ridondante: il carico di rete non ha altro a cui rivolgersi a causa dell'utilizzo, il che si traduce in una capacità insufficiente per l'intera soluzione.

- Tempo di failover: il tempo di failover è il tempo impiegato da un componente secondario per assumere completamente il ruolo di componente principale. Il tempo di failover è legato a diversi fattori: il tempo necessario per rilevare l'errore, il tempo necessario per abilitare la connettività secondaria e il tempo necessario per notificare la modifica al resto della rete. Il rilevamento degli errori può essere migliorato utilizzando Dead Peer Detection (DPD) per VPN i link e Bidirectional Forwarding Detection () per i link. BFD AWS Direct Connect Il tempo necessario per abilitare la connettività secondaria può essere molto breve (se queste connessioni sono sempre attive), può essere breve (se è necessario abilitare una VPN connessione preconfigurata) o più lungo (se è necessario spostare risorse fisiche o configurare nuove risorse). La notifica al resto della rete avviene in genere tramite protocolli di routing all'interno della rete del cliente, ognuno dei quali ha tempi di convergenza e opzioni di configurazione diversi: la configurazione di questi non rientra nell'ambito di questo white paper.
- Ingegneria del traffico: l'ingegneria del traffico nel contesto della progettazione resiliente della connettività di rete ibrida mira a definire il modo in cui il traffico dovrebbe fluire su più connessioni disponibili in scenari normali e di guasto. Si consiglia di seguire il concetto di progettazione in caso di errore, in cui è necessario esaminare come funzionerà la soluzione in diversi scenari di errore e se sarà accettabile per l'azienda o meno. Questa sezione illustra alcuni dei casi d'uso più comuni di ingegneria del traffico che mirano a migliorare il livello di resilienza complessivo della soluzione di connettività di rete ibrida. La AWS Direct Connect sezione dedicata al routing BGP illustra diverse opzioni di ingegneria del traffico per influenzare il flusso del traffico (comunità, preferenze BGP locali, lunghezza del percorso AS). Per progettare una soluzione di ingegneria del traffico efficace, è necessario avere una buona conoscenza di come ciascuno dei componenti di AWS rete gestisce il routing IP in termini di valutazione e selezione del percorso, nonché dei possibili meccanismi per influenzare la selezione del percorso. I dettagli in merito non rientrano nell'ambito di questo documento. Per ulteriori informazioni, consulta Transit Gateway Route Evaluation Order, Site-to-Site VPNRoute Priority e Direct Connect Routing e BGP la documentazione necessaria.

> **Note**
>
> Nella tabella delle VPC rotte, è possibile fare riferimento a un elenco di prefissi che contiene regole di selezione delle rotte aggiuntive. Per ulteriori informazioni su questo caso d'uso, consulta la priorità delle rotte per gli elenchi di prefissi. AWS Transit Gateway Le tabelle di routing supportano anche gli elenchi di prefissi, ma una volta applicate vengono estese a voci di percorso specifiche.

Esempio di Site-to-Site VPN connessioni doppie con percorsi più specifici

Questo scenario si basa su un piccolo sito locale che si connette a un unico Regione AWS sito tramite VPN connessioni ridondanti via Internet a. AWS Transit Gateway Il progetto di ingegneria del traffico illustrato nella Figura 10 mostra che con l'ingegneria del traffico è possibile influenzare la selezione del percorso che aumenta l'affidabilità della soluzione di connettività ibrida mediante:

- Connettività ibrida resiliente: tutte VPN le connessioni ridondanti offrono la stessa capacità prestazionale, supportano il failover automatico utilizzando il protocollo di routing dinamico (BGP) e velocizzano il rilevamento degli errori di connessione utilizzando il rilevamento «dead peer». VPN
- Efficienza delle prestazioni: la configurazione ECMP su entrambe le VPN connessioni AWS Transit Gateway aiuta a massimizzare la larghezza di banda complessiva della connessione. VPN In alternativa, pubblicizzando percorsi diversi e più specifici insieme al percorso di riepilogo del sito, è possibile gestire il carico in modo indipendente tra le due connessioni VPN

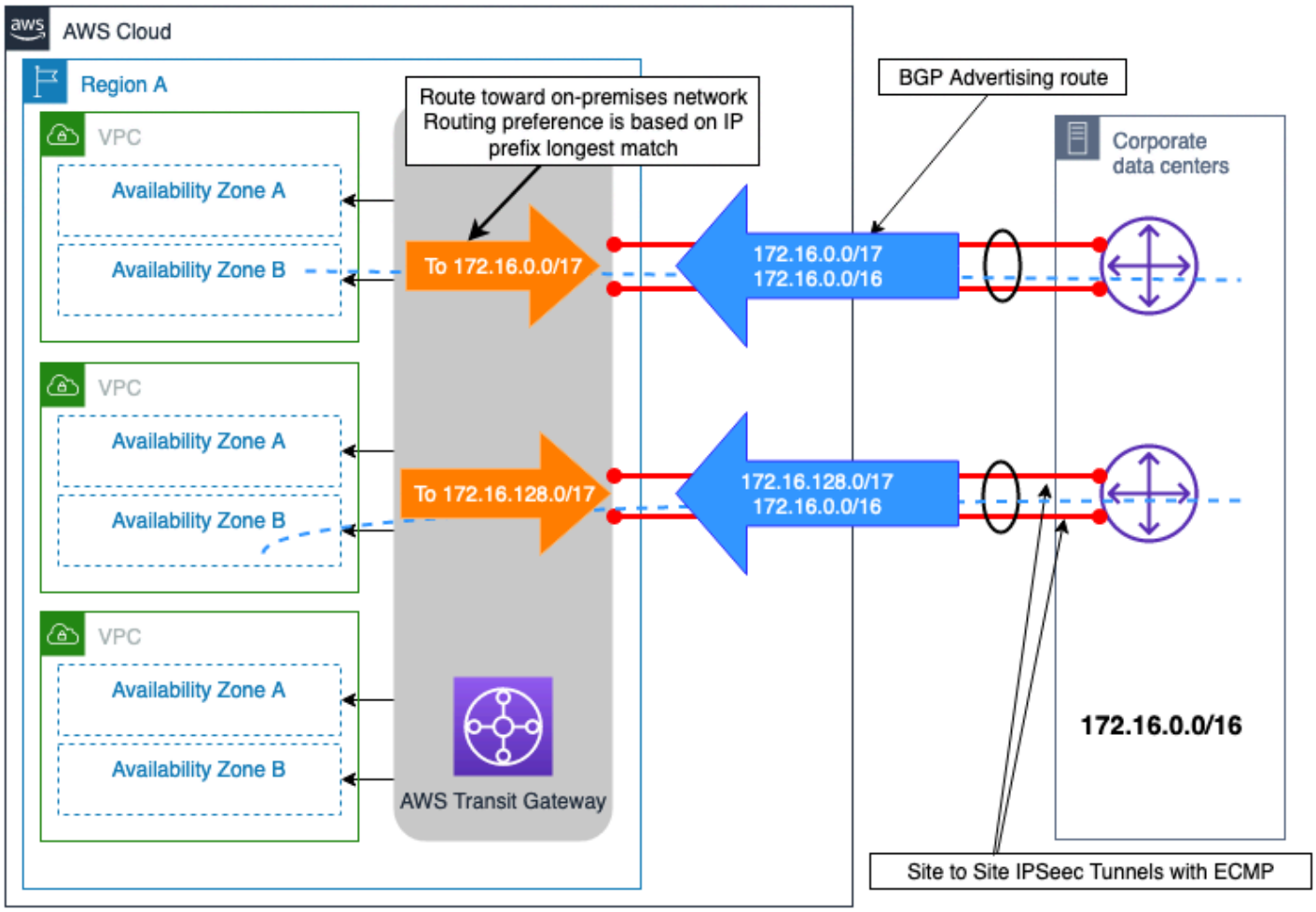

Figura 10 — Esempio di Site-to-Site VPN connessioni doppie con percorsi più specifici

Esempio di due siti locali con più connessioni DX

Lo scenario illustrato nella Figura 11 mostra due siti di data center locali situati in diverse regioni geografiche e collegati tramite il modello di connettività Maximum Resiliency (descritto nelle Raccomandazioni sulla AWS Direct Connect resilienza) AWS utilizzando with and. AWS Direct Connect DXGW VGW Questi due siti locali sono interconnessi tra loro tramite un collegamento di interconnessione del data center (). DCI I prefissi IP locali (192.168.0.0/16) che appartengono alle filiali remote vengono pubblicizzati da entrambi i siti dei data center locali. Il percorso principale per questo prefisso deve essere il data center 1. Il traffico da e verso le filiali remote verrà eseguito il failover verso il data center 2 in caso di guasto del data center 1 o di entrambe le sedi DX. Inoltre, esiste un prefisso IP specifico del sito per ogni data center. Questi prefissi devono essere raggiunti direttamente e tramite l'altro sito del data center in caso di guasto in entrambe le sedi DX.

Associando gli attributi BGP Community alle rotte pubblicizzate AWS DXGW, è possibile influenzare lateralmente la selezione del percorso di uscita. AWS DXGW Questi attributi comunitari controllano AWS l'attributo BGP Local Preference assegnato al percorso pubblicizzato. Per ulteriori informazioni, consulta le politiche e le AWS community di DX Routing. BGP

Per massimizzare l'affidabilità della connettività a Regione AWS livello, ogni coppia di connessioni AWS DX viene configurata in ECMP modo che entrambe possano essere utilizzate contemporaneamente per il trasferimento di dati tra ogni sito locale e. AWS

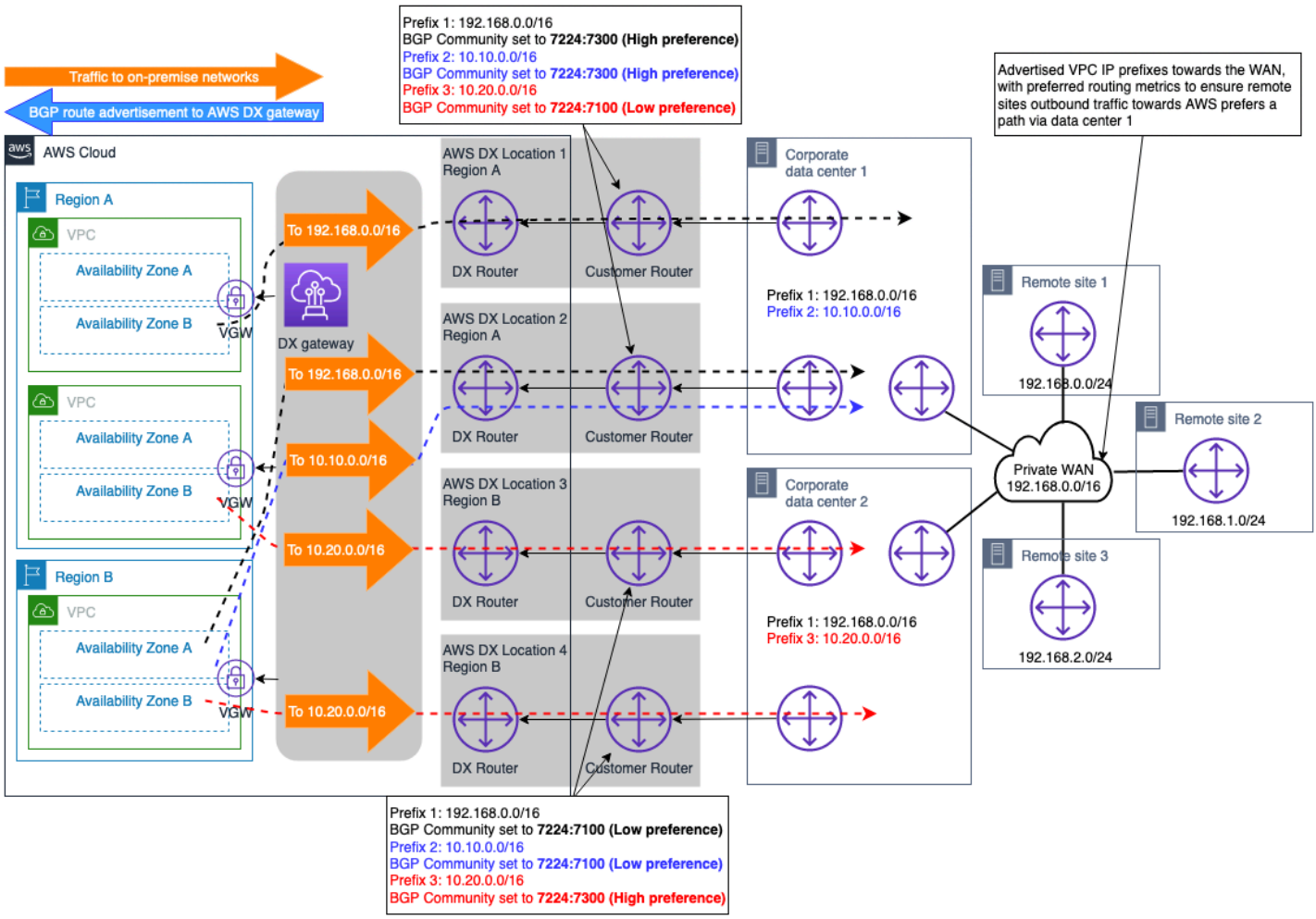

Figura 11 — Esempio di due siti locali con più connessioni DX

Con questo design, i flussi di traffico destinati alle reti locali (con la stessa lunghezza del prefisso e la stessa BGP community pubblicizzati) verranno distribuiti tra le doppie connessioni DX utilizzate dal sito. ECMP Tuttavia, se non ECMP è richiesto attraverso la connessione DX, lo stesso concetto discusso in precedenza e descritto nella documentazione BGPsulle politiche e le comunità di routing può essere utilizzato per progettare ulteriormente la selezione del percorso a livello di connessione DX.

Nota: se nel percorso all'interno dei data center locali sono presenti dispositivi di sicurezza, questi dispositivi devono essere configurati per consentire ai flussi di traffico in uscita da un collegamento DX e provenienti da un altro collegamento DX (entrambi i collegamenti utilizzatiECMP) all'interno dello stesso sito del data center.

VPNconnessione come esempio di connessione di backup a DX AWS

VPNpuò essere selezionato per fornire una connessione di rete di backup a una AWS Direct Connect connessione. In genere, questo tipo di modello di connettività è determinato dal costo, in quanto offre un livello di affidabilità inferiore alla soluzione complessiva di connettività ibrida a causa delle prestazioni indeterministiche su Internet, e non SLA è possibile ottenere una connessione tramite la rete Internet pubblica. È un modello di connettività valido ed economico e deve essere utilizzato quando il costo è la priorità assoluta e il budget è limitato, o magari come soluzione provvisoria fino al provisioning di un DX secondario. La Figura 12 illustra la progettazione di questo modello di connettività. Una considerazione fondamentale di questa progettazione, in cui entrambe le connessioni VPN e DX terminano in corrispondenza del AWS Transit Gateway, è che la VPN connessione può annunciare un numero maggiore di rotte rispetto a quelle che possono essere pubblicizzate tramite una connessione DX a cui è connessa. AWS Transit Gateway Ciò può causare una situazione di routing non ottimale. Un'opzione per risolvere questo problema consiste nel configurare il filtraggio delle rotte sul dispositivo gateway del cliente (CGW) per le rotte ricevute dalla VPN connessione, consentendo l'accettazione solo delle rotte di riepilogo.

Nota: per creare il percorso di riepilogo su AWS Transit Gateway, è necessario specificare un percorso statico verso un allegato arbitrario nella tabella delle rotte in modo che il riepilogo venga inviato lungo il AWS Transit Gateway percorso più specifico.

Dal punto di vista della tabella di AWS Transit Gateway routing, le rotte per il prefisso locale vengono ricevute sia dalla connessione AWS DX (viaDXGW) che daVPN, con la stessa lunghezza del prefisso. Seguendo la logica di priorità del percorso di AWS Transit Gateway, le rotte ricevute tramite Direct Connect hanno una preferenza maggiore rispetto a quelle ricevute su Site-to-SiteVPN, e quindi il percorso su di AWS Direct Connect sarà il preferito per raggiungere le reti locali.

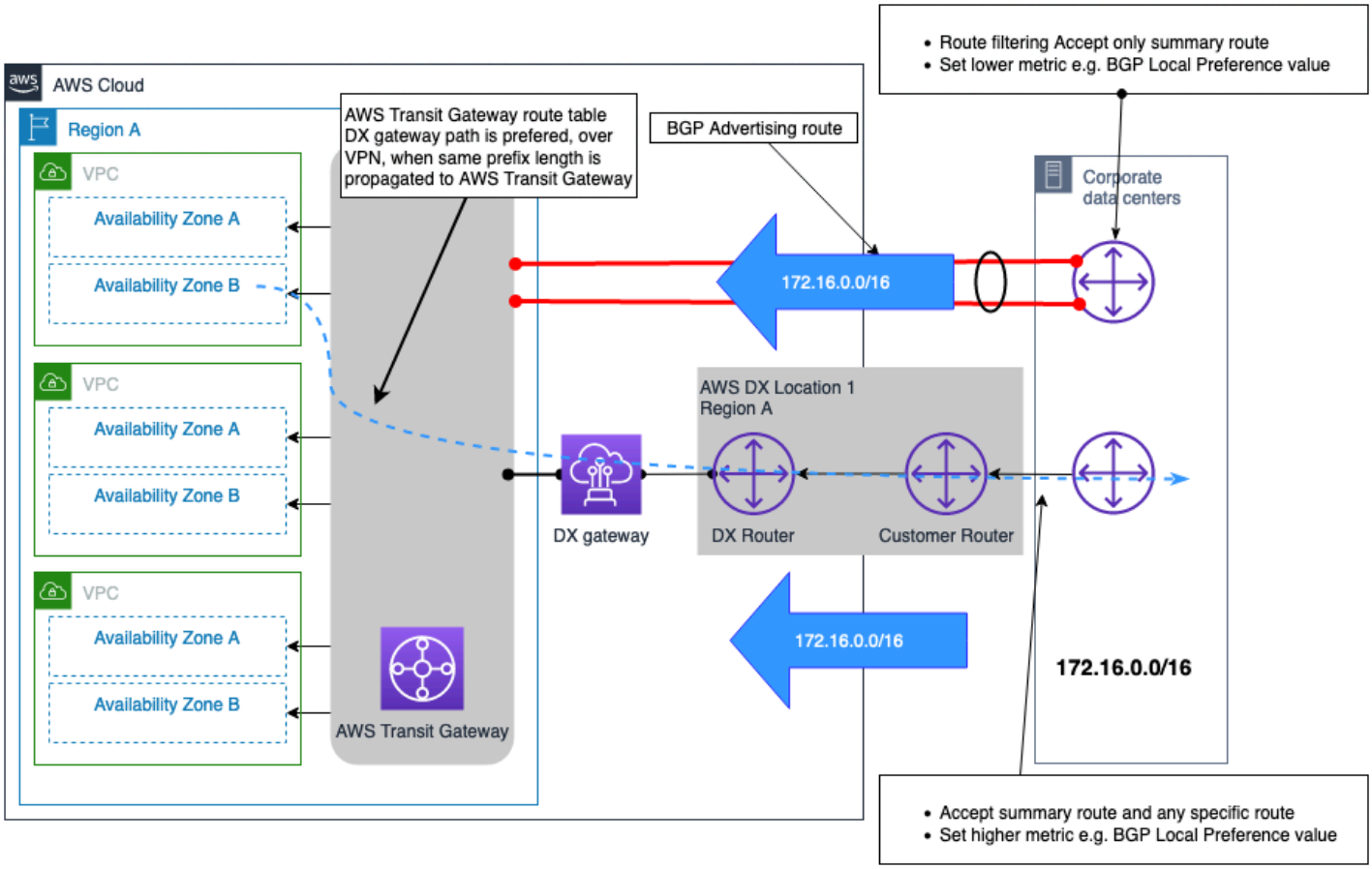

Figura 12 — esempio di VPN connessione come backup su AWS DX

Il seguente albero decisionale guida l'utente nel prendere la decisione desiderata per ottenere una connettività di rete ibrida resiliente (che si tradurrà in una connettività di rete ibrida affidabile). Per ulteriori informazioni, consulta AWS Direct Connect Resiliency Toolkit.

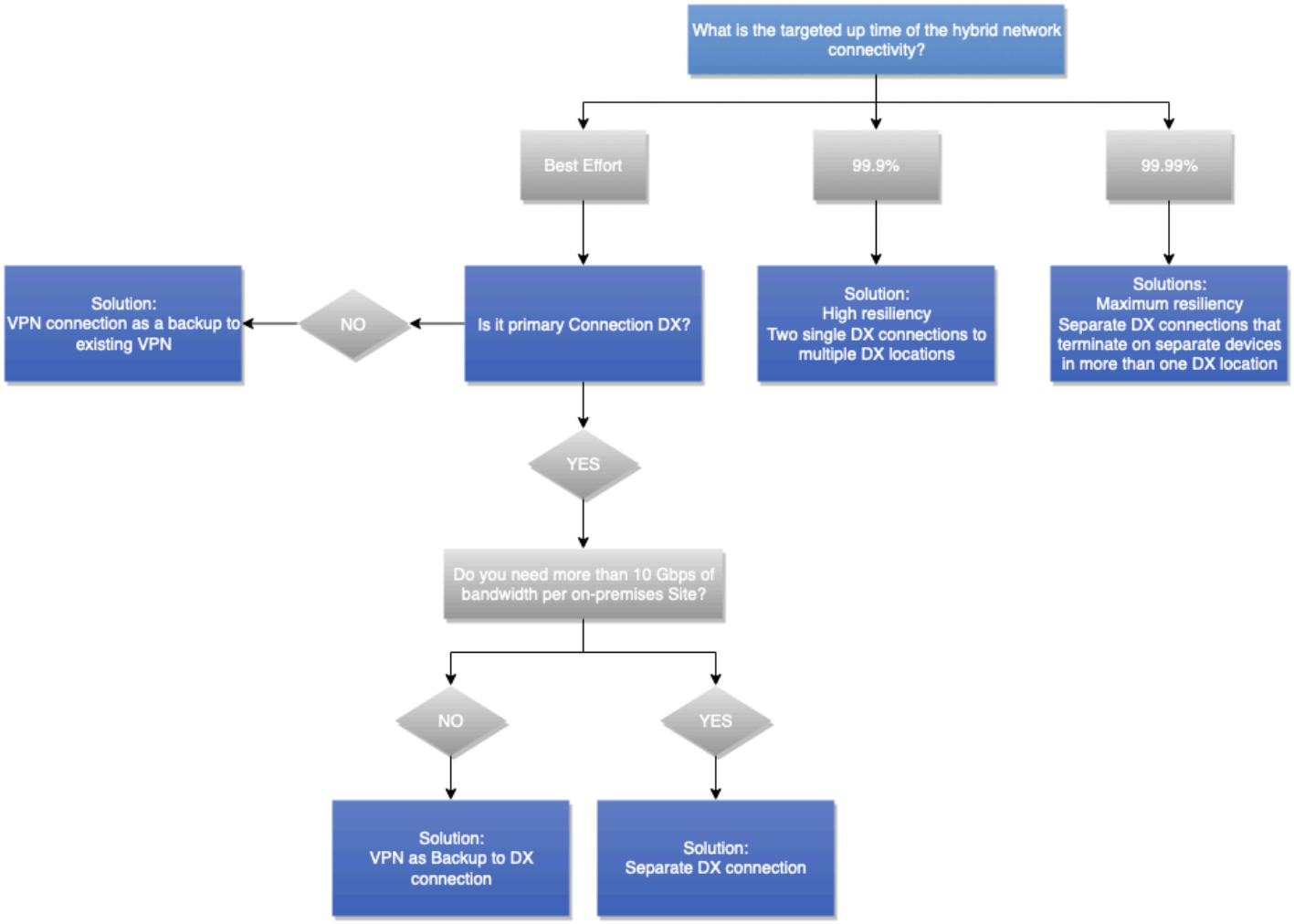

Figura 13 — Albero decisionale sull'affidabilità

Gestito dal cliente VPN e SD- WAN

Definizione

La connettività a Internet è un bene di prima necessità e la larghezza di banda disponibile continua ad aumentare ogni anno. Alcuni clienti scelgono di creare un sistema virtuale basato WAN su Internet invece di crearne e gestirne uno privato. WAN Una rete geografica definita dal software (SD-WAN) consente alle aziende di fornire e gestire in modo rapido e centralizzato questo ambiente virtuale WAN attraverso un uso intelligente del software. Altri clienti scelgono di adottare la tradizionale gestione autonoma da sito a sito. VPNs

Impatto sulle decisioni di progettazione

La gestione SD WAN e quella gestita dal cliente VPNs possono essere eseguite su Internet o. AWS Direct Connect SD- WAN (o qualsiasi altro VPN overlay software) è affidabile quanto il trasporto di rete sottostante. Pertanto, l'affidabilità e SLA le considerazioni discusse in precedenza in questo white paper sono applicabili qui. Ad esempio, la creazione di un WAN overlay SD su Internet non offrirà la stessa affidabilità rispetto a una sovrapposizione basata su un. AWS Direct Connect

Definizione dei requisiti

- Utilizzi SD- WAN nella tua rete locale?
- Sono necessarie funzionalità specifiche che sono disponibili solo su alcune appliance virtuali utilizzate per la VPN terminazione?

Soluzioni tecniche

AWS consiglia l'integrazione di SD- WAN con AWS Transit Gateway e pubblica un elenco dei fornitori che supportano l'integrazione. AWS Transit Gateway AWS può fungere da hub per i WAN siti SD o da sito parlato. La AWS backbone può essere utilizzata per connettere diversi WAN hub SD distribuiti all'interno AWS di una rete altamente affidabile e performante. WANLe soluzioni SD supportano il failover automatizzato attraverso qualsiasi percorso disponibile, funzionalità aggiuntive di monitoraggio e osservabilità in un unico pannello di gestione. L'ampio uso della configurazione e dell'automazione automatiche consente un approvvigionamento e una visibilità rapidi rispetto ai sistemi tradizionaliWANs. Tuttavia, l'uso del tunneling e dei costi generali di crittografia non è paragonabile ai collegamenti in fibra dedicati e ad alta velocità utilizzati nella connettività privata.

In alcuni casi, è possibile scegliere di utilizzare un'appliance virtuale dotata di funzionalità. VPN I motivi per scegliere un'appliance virtuale autogestita includono caratteristiche tecniche e compatibilità con il resto della rete. Quando si seleziona una WAN soluzione autogestita VPN o SD che utilizza un'appliance virtuale distribuita in un'EC2istanza, l'utente è responsabile della gestione di tale appliance. L'utente è inoltre responsabile dell'elevata disponibilità e del failover tra le appliance virtuali. Tale progettazione aumenta la responsabilità operativa; tuttavia, potrebbe offrirvi maggiore flessibilità. Le caratteristiche e le funzionalità della soluzione dipendono dall'appliance virtuale selezionata.

Marketplace AWS contiene molte appliance VPN virtuali che i clienti possono implementare su AmazonEC2. AWS consiglia di iniziare con S2S AWS gestito VPN e di esaminare altre opzioni se

non soddisfa i tuoi requisiti. Il sovraccarico di gestione delle appliance virtuali è responsabilità del cliente.

Esempio di utilizzo nel settore automobilistico di Example Corp.

Questa sezione del white paper illustra come le considerazioni, le domande sulla definizione dei requisiti e gli alberi decisionali vengono utilizzati per aiutarvi a decidere la progettazione ottimale della rete ibrida. L'identificazione e l'acquisizione dei requisiti sono importanti poiché vengono utilizzati come input per gli alberi decisionali. L'acquisizione anticipata dei requisiti evita ulteriori iterazioni di progettazione. L'interruzione totale di un progetto, se è necessario rivisitare il progetto e disporre di risorse preziose, può essere ridotto al minimo e idealmente evitato quando i requisiti vengono compresi in anticipo.

In questa sezione verrà utilizzato Example Corp. Automotive come cliente illustrativo. Stanno cercando di implementare inizialmente il loro primo progetto di analisi su. AWS Il progetto di analisi si concentra sull'analisi dei dati delle auto prodotte dall'azienda e di altri set di dati già esistenti nei data center dell'azienda. Inizialmente, il gruppo di architettura dell'azienda ritiene che avranno bisogno di un Account AWS Amazon VPC e di poche sottoreti per ospitare ambienti di produzione e sviluppo. Il team di progetto non vede l'ora di iniziare e ha richiesto l'accesso all'ambiente di sviluppo il prima possibile. Il loro obiettivo è entrare in produzione tra tre mesi.

Example Corp. Automotive prevede inoltre di utilizzarlo AWS per diversi progetti aggiuntivi, come la migrazione dei propri sistemi ERP, della Virtual Desktop Infrastructure (VDI) e di altre 20 applicazioni dall'ambiente locale ai AWS prossimi 6 mesi. Alcuni requisiti per progetti aggiuntivi sono ancora in fase di definizione, ma è chiaro che il loro Cloud AWS utilizzo è destinato a crescere.

Il team di architettura ha deciso di sfruttare l'approccio descritto in questo white paper. Hanno utilizzato le domande sulla definizione dei requisiti delineate in ciascuna considerazione per acquisire gli input necessari per prendere le decisioni di progettazione.

Iniziano con i requisiti relativi al tipo di connettività, riassunti nella tabella seguente.

Tabella 4 — Esempi di input di affidabilità di Automotive Corp.

Considerazioni sulla selezione del tipo di connettività	Domande sulla definizione dei requisiti	Risposte
È ora di implementare	Qual è la tempistica richiesta per l'implementazione? Ore, giorni, settimane o mesi?	• Sviluppo/Test: 1 mese • Produzione: 3 mesi
Sicurezza	I requisiti e le politiche di sicurezza consentono l'utilizzo di connessioni crittografate su Internet per connettersi AWS o impongono l'utilizzo di connessioni di rete private?	• Sviluppo/Test: VPN da sito a sito accettabile • Produzione: è richiesta una rete privata
	Quando si utilizzano connessioni di rete private, il livello di rete deve fornire la crittografia in transito?	No, verrà utilizzata la crittografia a livello di applicazione.
SLA	È richiesto uno SLA di connettività ibrida con crediti di servizio?	• Sviluppo/Test: No • Produzione: Sì
	Qual è l'obiettivo di uptime?	• Sviluppo/Test: N/A • Produzione: 99,99%
	L'intera rete ibrida rispetta l'obiettivo di uptime?	• Sviluppo/Test: N/A • Produzione: Sì
Prestazioni	Qual è la produttività richiesta ?	• Sviluppo/Test: 100 Mbps • Produzione: 500 Mbps, crescita fino a 2 Gbps
	Qual è la latenza massima accettabile tra la rete locale AWS e quella locale?	• Sviluppo/Test: nessun requisito rigido • Produzione: meno di 30 ms

Considerazioni sulla selezione del tipo di connettività	Domande sulla definizione dei requisiti	Risposte
	Qual è il jitter di rete massimo accettabile?	• Sviluppo/Test: nessun requisito rigido • Produzione: jitter minimo richiesto
Costo	A quanti dati invieresti AWS al mese?	• Sviluppo/Test: 2 TB • Produzione: 20 TB, crescita fino a 50 TB
	Da quanti dati invieresti AWS al mese?	• Sviluppo/Test: 1 TB • Produzione: da 10 TB a 25 TB
	Questa connettività è permanente?	Sì

In base ai requisiti ricevuti, il team di architettura ha seguito l'albero decisionale sul tipo di connettività riportato nella Figura 9. Ha consentito al team di architettura di decidere il tipo di connettività per gli ambienti di sviluppo, test e produzione. Per quanto riguarda l'ambiente di produzione, hanno considerato i requisiti immediati e quelli imminenti. Per lo sviluppo e il test Example Corp. Automotive stabilirà una site-to-site VPN su Internet. Per la produzione, collaboreranno con un fornitore di servizi a cui connettere la rete aziendale. AWS Direct Connect Example Corp. Automotive inizialmente aveva preso in considerazione l'utilizzo di una connessione ospitata Direct Connect, tuttavia, a causa dei requisiti per uno SLA AWS fornito, ha scelto Direct Connect Dedicated Connections.

Dopo aver deciso il tipo di connettività, il passaggio successivo consiste nell'individuare i requisiti che influiscono sulla selezione del progetto di connettività. Ciò è correlato alla progettazione logica, ad esempio alla modalità di configurazione delle connessioni e ai AWS servizi da utilizzare per supportare i requisiti aziendali e tecnici.

Per comprendere i requisiti del modello di scalabilità e comunicazione, il team di architettura ha utilizzato le domande sulla definizione dei requisiti contenute nelle sezioni associate di questo white paper. I requisiti relativi a queste due considerazioni sono riassunti nella tabella seguente.

Tabella 5 — Domande sulla definizione dei requisiti

Considerazioni sulla selezione del progetto di connettività	Domande sulla definizione dei requisiti	Risposte
Scalabilità	Qual è il numero attuale o previsto di VPC che richiedono la connettività ai siti locali?	2 inizialmente, con un aumento fino a 30 in 6 mesi
	Questi VPC sono distribuiti in una Regione AWS o più regioni?	Regione singola
	A quanti siti locali è necessario connettersiAWS?	2 data center
	A quanti dispositivi Customer Gateway avete, per sito, a cui dovete connetterviAWS?	2 router per data center
	Quanti percorsi dovrebbero essere pubblicizzati AWS sui VPC e il numero di percorsi previsti che verranno ricevuti da Side? AWS	• Percorsi da pubblicizzare su: 20 percorsi AWS • Percorsi da ricevere da AWS: 1 /16 percorso
	Si prevede di prendere in considerazione l'aumento della larghezza di banda della connessione AWS nelle prossime future?	• Sviluppo/Test: 100 Mbps • Produzione: 500 Mbps, crescita fino a 2 Gbps.
Modelli di progettazione della connettività	È necessario abilitare la comunicazione tra VPC (all'interno di una regione e/o tra regioni)?	Sì, entro un Regione AWS
	È necessario accedere ai servizi di endpoint AWS	Sì

Considerazioni sulla selezione del progetto di connettività	Domande sulla definizione dei requisiti	Risposte
	pubblici direttamente dall'ambiente locale?	
	È necessario accedere ai AWS servizi utilizzando gli endpoint VPC dall'ambiente locale?	No

Sulla base degli input, il team di architettura ha seguito l'albero decisionale della sezione Connectivity Design. Dopo aver previsto che il numero di VPC aumenterà da 2 a 30 nei prossimi 6 mesi, il team di architettura ha deciso di utilizzarlo AWS Transit Gateway come gateway di terminazione per la connessione e per il routing tra VPC. Independent AWS Transit Gateway s interromperà la connessione VPN utilizzata per lo sviluppo e il test e per la connettività di produzione con. AWS Direct Connect L'utilizzo di AWS Transit Gateway s separati semplifica la gestione delle modifiche e fornisce una chiara demarcazione tra ambienti di sviluppo/test e di produzione. Per la produzione, è necessario un gateway a causa di. AWS Direct Connect AWS Transit Gateway Verrà utilizzata una VIF pubblica per accedere ai servizi di endpoint AWS pubblici. La Figura 14 illustra il percorso seguito nell'albero decisionale in base ai requisiti raccolti.

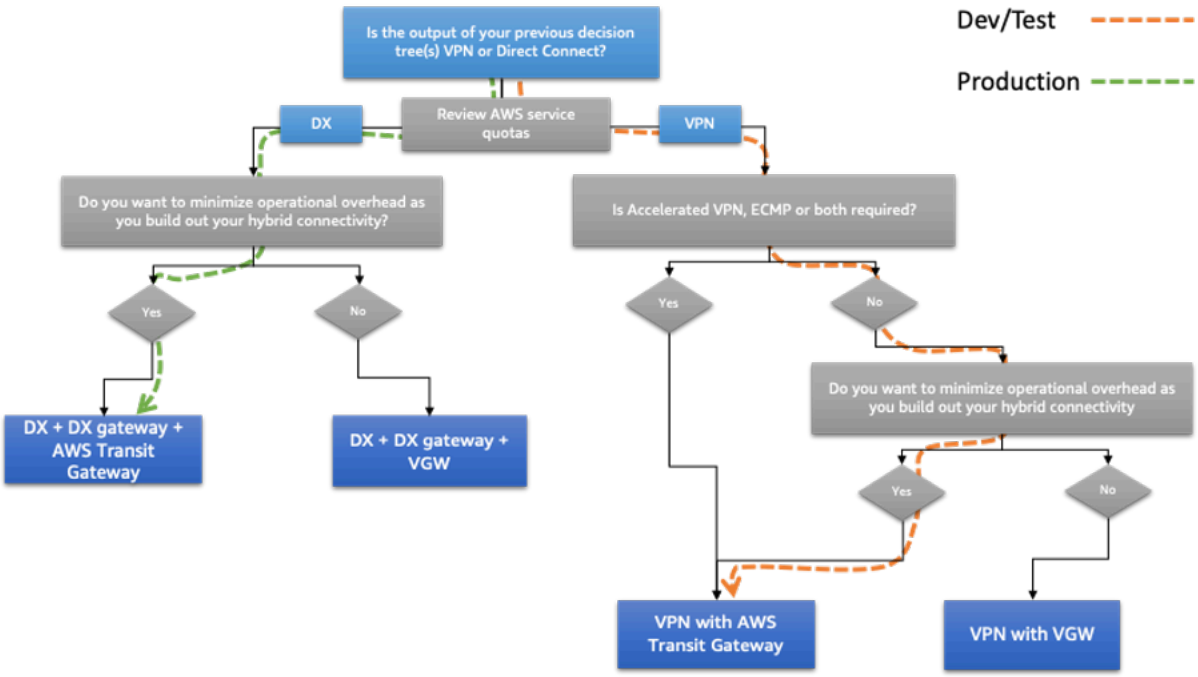

Figura 14 — Albero decisionale per la progettazione di connessioni automobilistiche di Example Corp.

Dopo aver deciso la soluzione per soddisfare i requisiti del modello di scalabilità e comunicazione, il passaggio successivo consiste nell'acquisire i requisiti associati all'affidabilità. Ciò è correlato al livello di disponibilità e resilienza richiesto.

Per acquisire i requisiti di affidabilità, il team di architettura ha utilizzato le domande sulla definizione dei requisiti contenute nella sezione associata di questo white paper. I requisiti sono riassunti nella tabella seguente.

Tabella 6 — Domande sui requisiti di affidabilità

Considerazioni sulla selezione del progetto di connettività	Domande sulla definizione dei requisiti	Risposte
Affidabilità	Qual è l'entità dell'impatto sull'azienda in caso di interruzione della connettività? AWS	• Sviluppo/Test: basso • Produzione: alta
	Dal punto di vista aziendale, il costo derivante da un guasto di connettività AWS supera il costo dell'implementazione di un modello di connettività altamente affidabile? AWS	• Sviluppo/Test: No • Produzione: Sì

Sulla base degli input ricevuti, il team di architettura ha seguito l'albero decisionale riportato nelle sezioni sulle considerazioni sull'affidabilità trattate in precedenza in questo white paper. Dopo aver considerato l'obiettivo di uptime del 99,99% per la connettività di produzione e l'elevato impatto aziendale in caso di interruzione del servizio, il team di architettura ha deciso di utilizzare 2 sedi Direct Connect e disporre di 2 collegamenti da ciascun data center locale a ciascuna sede Direct Connect (4 collegamenti in totale). La connettività VPN utilizzata per lo sviluppo e il test utilizzerà anche due connessioni VPN per una ridondanza aggiuntiva. Utilizzando le tecniche di ingegneria dei percorsi discusse nella sezione sull'affidabilità, la connettività verrà configurata come segue:

- Per lo sviluppo e il test, il traffico verrà bilanciato dal carico utilizzando ECMP sui 2 tunnel diretti al data center principale. Ciò consente un throughput più elevato. I tunnel che portano al data center secondario verranno utilizzati in caso di guasto dei tunnel primari.
- Per la produzione, la latenza tra locale e AWS su una delle due sedi Direct Connect è molto simile. In questo caso, è stato deciso di bilanciare il carico del traffico tra AWS e in locale sulle due connessioni dirette al data center primario per i sistemi locali distribuiti nel data center primario. Analogamente, per i sistemi locali in esecuzione nel data center secondario, il carico del traffico verrà bilanciato tra le due connessioni al data center secondario. In caso di guasto delle connessioni, BGP faciliterà un failover automatico.

La Figura 15 illustra il percorso seguito nell'albero decisionale in base ai requisiti raccolti.

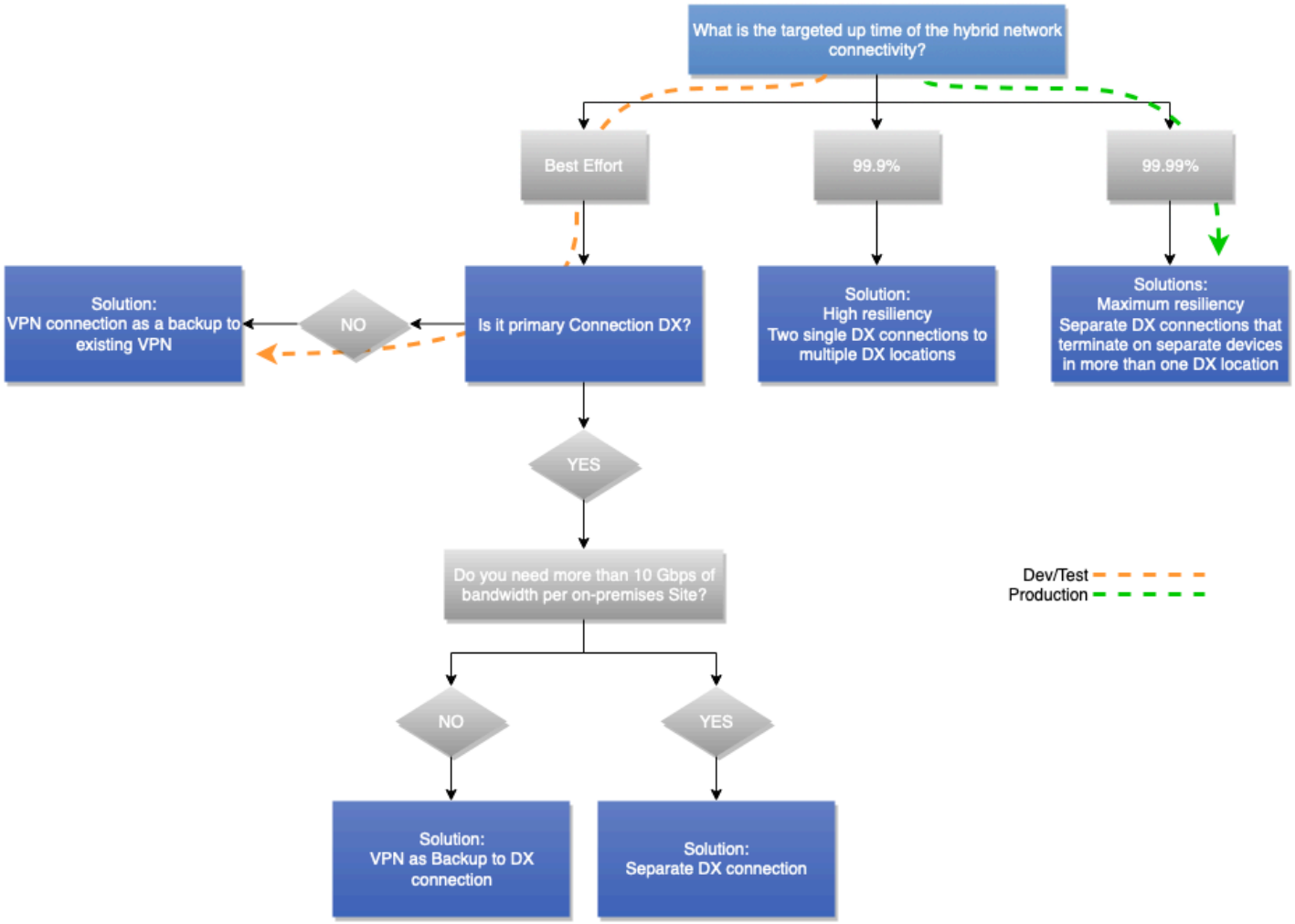

Figura 15 — Albero decisionale sull'affidabilità del settore automobilistico di Example Corp.

Architettura selezionata da Example Corp. Automotive

Il diagramma seguente illustra l'architettura selezionata da Example Corp. Automotive dopo aver raccolto i requisiti e aver esplorato gli alberi decisionali descritti nelle sezioni precedenti di questo white paper.

Utilizza la VPN AWS S2S su Internet e termina per lo sviluppo e il test. AWS Transit Gateway Viene quindi utilizzato AWS Direct Connect con il gateway Direct Connect e un secondo AWS Transit Gateway per il traffico di produzione. AWS Transit Gatewayviene utilizzato per il routing tra VPC. Dal punto di vista del percorso dei dati, i tunnel VPN per il data center primario vengono utilizzati come percorsi primari per lo sviluppo e il test, mentre i tunnel verso il data center secondario vengono utilizzati come percorsi di failover. Per il traffico di produzione, tutte le connessioni vengono utilizzate contemporaneamente. Il traffico proveniente da AWS preferisce la connessione di rete più opzionale in base al data center in cui si trova il sistema locale. Example Corp. Automotive utilizza tecniche di progettazione dei percorsi simili per preferire il percorso appropriato quando viene inviato il traffico e AWS garantire che vengano utilizzati percorsi di traffico simmetrici per ridurre al minimo l'uso della rete aziendale tra i data center primari e secondari locali.

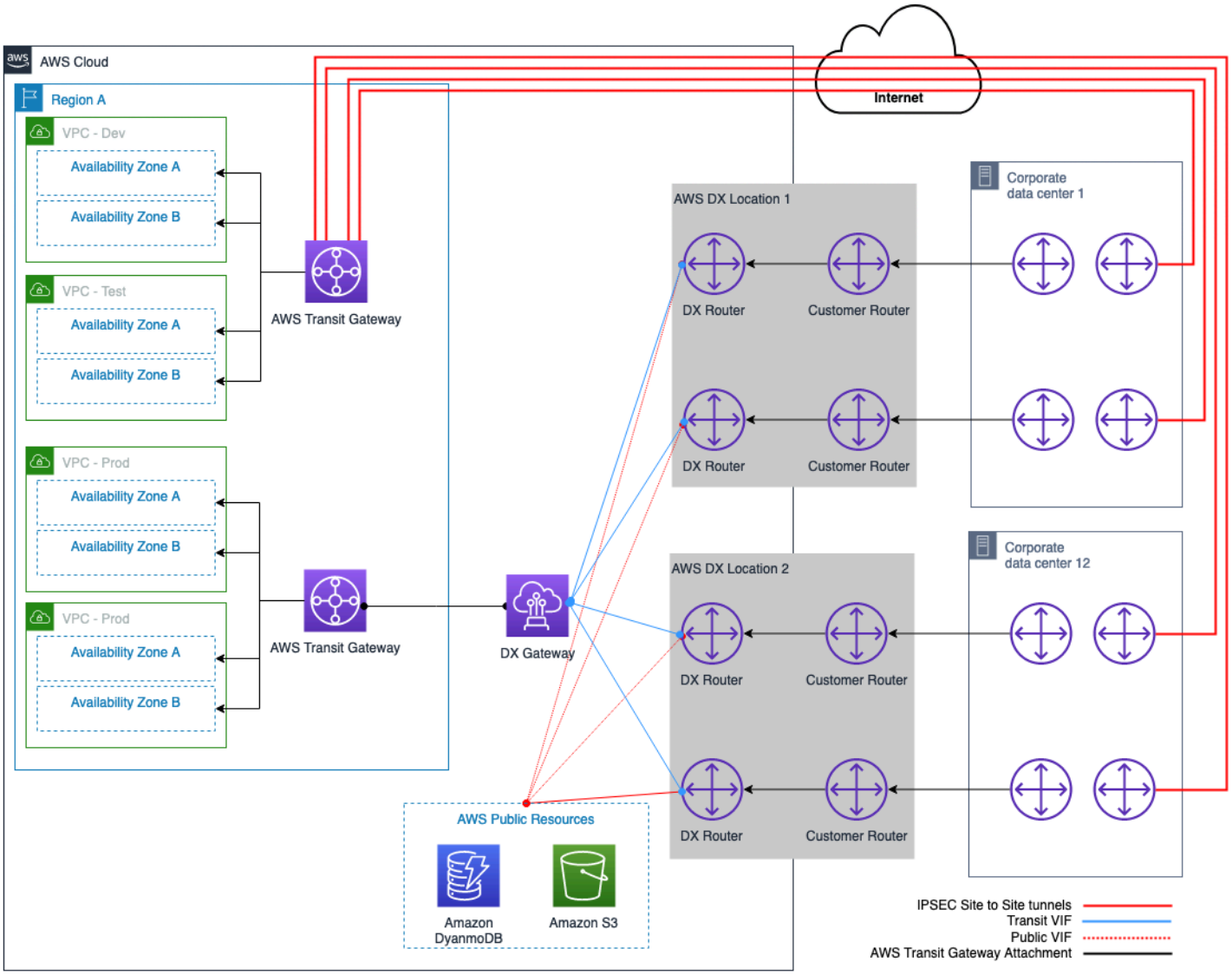

Figura 16 — Modello di connettività ibrida selezionato da Example Corp. Automotive

Conclusioni

Un modello di connettività ibrida è uno dei punti di partenza fondamentali per l'adozione del cloud computing. Una rete ibrida può essere costruita con un'architettura ottimale seguendo il processo di selezione del modello di connettività descritto in questo white paper.

Il processo consiste in considerazioni disposte in ordine logico. L'ordine ricorda da vicino un modello mentale seguito da architetti esperti di rete e cloud. All'interno di ogni gruppo di considerazioni, gli alberi decisionali consentono una rapida selezione del modello di connettività, anche con requisiti di input limitati. È possibile che alcune considerazioni e gli impatti corrispondenti indichino soluzioni diverse. In questi casi, in qualità di decisori, potrebbe essere necessario scendere a compromessi su alcuni requisiti e selezionare la soluzione più ottimale che soddisfi i requisiti aziendali e tecnici.

Fattori determinanti

I contributori a questo documento includono:

- James Devine, Architetto principale delle soluzioni, Amazon Web Services
- Andrew Gray, Architetto principale delle soluzioni — Reti, Amazon Web Services
- Maks Khomutskyi, Architetto di soluzioni senior, Amazon Web Services
- Marwan Al Shawi, architetto di soluzioni, Amazon Web Services
- Santiago Freitas, responsabile della tecnologia, Amazon Web Services
- Evgeny Vaganov, architetto specializzato in soluzioni di rete, Amazon Web Services
- Tom Adamski, architetto specializzato in soluzioni di rete, Amazon Web Services
- Armstrong Onaiwu, architetto di soluzioni, Amazon Web Services

Approfondimenti

- Realizzazione di un'infrastruttura di reti AWS multi-VPC sicura e scalabile
- Opzioni DNS cloud ibrido per Amazon VPC
- Opzioni di connettività di Amazon Virtual Private Cloud
- Documentazione di Amazon Virtual Private Cloud
- Documentazione AWS Direct Connect
- Qual è la differenza tra un'interfaccia virtuale ospitata (VIF) e una connessione ospitata?

Revisioni del documento

Per ricevere una notifica sugli aggiornamenti del white paper, è possibile iscriversi al feed RSS.

Modifica	Descrizione	Data
Aggiornamento minore	Aggiornato per riflettere l'aumento del limite di quota DX.	10 luglio 2023
Aggiornamento importante	Aggiornato per incorporare le migliori pratiche, servizi e funzionalità più recenti.	6 luglio 2023
Aggiornamento minore	Diagrammi di architettura di riferimento aggiornati per riflettere le modifiche nella quota DX.	27 giugno 2023
Aggiornamento minore	Collegamenti interrotti fissi.	22 marzo 2022
Pubblicazione iniziale	Whitepaper pubblicato per la prima volta	22 settembre 2020

Note

I clienti hanno la responsabilità di effettuare la propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWSi prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.