

# Jornadas Digitais CCTD

## Nuvem Híbrida

---

# #7





# Programação

- Retrospectiva
- Palestra
- Perguntas
- Encerramento e convite para próximo

A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a dark green background, resembling a circuit board or a neural network.

# Retrospectiva

---



CENTRO DE COMPETÊNCIA PARA  
TRANSFORMAÇÃO DIGITAL DO CEARÁ

## Objetivo

O objetivo do CCTD, enquanto programa de coordenação de políticas públicas, é transformar o Ceará em uma referência na adoção da transformação digital para impacto no cidadão, ensino e empreendedorismo.

## Pilares do CCTD

Capacidades  
Governamentais

Secretaria do  
Planejamento e Gestão |  
Casa Civil

Startups e  
Empreendedorismo

Secretaria da Ciência,  
Tecnologia e Educação  
Superior (Secitece)

Pesquisa e  
Desenvolvimento

Fundação Cearense de  
Apoio ao  
Desenvolvimento  
Científico e Tecnológico  
(Funcap)

Formação de Pessoas

Secretaria do  
Desenvolvimento  
Econômico e Trabalho  
(Sedet)



# Agenda Jornadas Digitais

12 de agosto - ~~LGPD (Mariana Zonari e Fernando Gebara)~~

26 de agosto - ~~Ciencia de dados (Jairo da Silva Junior)~~

09 de setembro - ~~DevOps~~

23 de setembro - ~~Estratégias de Migração para a nuvem~~

07 de outubro - ~~Modernização de Backup~~

21 de outubro - ~~Experiencia do Usuário (UX)~~

11 de novembro - **Nuvem híbrida**

25 de novembro - Containers

08 de dezembro - Inteligencia Artificial e aprendizagem de máquina



# Quem participa das Jornadas Digitais?

O público-alvo é composto por servidores concursados e terceirizados da área de TI das Secretarias, vinculadas e agencias reguladoras do estado do Ceará.

**Convide as outras pessoas da sua equipe!**

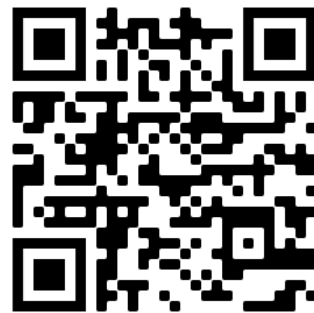


# CERTIFICAÇÕES

- A certificação será realizada da seguinte maneira:
  - Ao final das 10 palestras das Jornadas Digitais será disponibilizado na plataforma da Escola de Gestão Pública ([ava.egp.ce.gov.br/2019/](http://ava.egp.ce.gov.br/2019/)), para o participante, um certificado contendo a carga horária total das palestras que o mesmo participou;
  - Para tanto é preciso ter no **mínimo 70%** da carga horária de cada encontro;
  - Todos que atenderem os critérios da certificação, receberão um e-mail com o passo a passo de acesso à plataforma.
- Caso o interessado precise comprovar de imediato a sua participação em uma determinada palestra, poderá, também, solicitar a declaração, referente ao respectivo evento, por meio do e-mail **ava@egp.ce.gov.br**. O prazo para a devolutiva será em sete dias úteis após o recebimento do e-mail.
- Para demais esclarecimentos quanto à certificação, encaminhar e-mail para **ava@egp.ce.gov.br**.

# ONDE BUSCAR INFORMAÇÕES?

- No hot-site das Jornadas Digitais:
- <http://jornadasdigitais.cctd.ce.gov.br/>



## JORNADAS DIGITAIS



CENTRO DE COMPETÊNCIAS  
PARA TRANSFORMAÇÃO  
DIGITAL DO CEARÁ



Laboratório de  
Inovação e Dados



**CEARÁ**  
GOVERNO DO ESTADO  
SECRETARIA DO  
PLANEJAMENTO E GESTÃO

### Agenda Jornadas Digitais

12 de agosto - LGPD  
26 de agosto - Ciência de dados  
09 de setembro - DevOps  
23 de setembro - Estratégias de Migração para a nuvem  
07 de outubro - modernização de backup  
21 de outubro - Experiência do Usuário (UX)  
04 de novembro - Nuvem híbrida  
18 de novembro - Containers  
02 de dezembro - Inteligência Artificial e aprendizagem de máquina  
16 de dezembro - apps serverless

O Centro de Competências para a Transformação Digital do Estado do Ceará (CCTD-CE), em parceria com a Amazon Web Services do Brasil (AWS) e a Escola de Gestão Pública do Estado do Ceará (EGPCE), oferece as Jornadas Digitais, uma série de eventos de aprimoramento técnico em nuvem.

**Quem deve participar:** O público-alvo é composto por servidores e empregados públicos e terceirizados da área de TI das secretarias, vinculadas e agências reguladoras do estado do Ceará.

A cada quinze dias temos uma nova palestra para ser ofertada, a próxima será sobre o assunto "DevOps" no dia 09 de setembro, às 15 horas.

**Para se inscrever nessa palestra, clique aqui.**

## Palestras

Veja as palestras e tenha acesso ao conteúdo. Informe o seu nome, sobrenome e e-mail para acessar as palestras.

💡 Clique nos botões abaixo para selecionar a palestra que você queira assistir.

## Para se inscrever na palestra, **CLIQUE AQUI**

### Sobre

O Centro de Competências para a Transformação Digital do Estado do Ceará (CCTD-CE), em parceria com a Amazon Web Services do Brasil (AWS) e a Escola de Gestão Pública do Estado do Ceará (EGPCE), oferece as Jomadas Digitais, uma série de eventos de aprimoramento técnico em nuvem. O sexto evento da série será uma palestra sobre o tema de **Experiência do Usuário**.

**Quem deve participar:** O público-alvo é composto por servidores e empregados públicos e terceirizados da área de TI das Secretarias, vinculadas e agências reguladoras do estado do Ceará.

### Palestrantes

#### **Georgia da Cruz Pereira – Professora adjunta da Universidade Federal do Ceará**

Georgia é doutora em Comunicação pela UFPE. Pesquisadora no LabGRIM (Laboratório da Relação Infância, Juventude e Mídia) e da Célula de Design e Multimídia - SMD UFC. Atua no eixo de Experiência do Usuário em projetos de Governo Digital, pelo Insight Data Science Lab (UFC) e Iris - Laboratório de Inovação e Dados do Governo do Estado do Ceará. Ministra disciplinas da área de comunicação, design e semiótica e realiza estudos nas áreas de Interação Humano-Computador, Comunicação, Tecnologia e Infância, Transformação

# Apresentação



**Kevin Lira**



**Karlos Correia**



**Convidado Misterioso**

# PREENCHA A AVALIAÇÃO!

- Ao final do webinar você vai receber um pedido de avaliação dos palestrantes, que será enviado amanhã no email de agradecimento.
- Dê o seu feedback para sabermos que você gostou e para podermos melhorar sempre!



# Jornadas Digitais #7 – Nuvem Híbrida

Arquiteturas Híbridas Entre seu DC e AWS

Karlos Correia — Arquiteto de Soluções

Kevin Lira — Arquiteto de soluções









# Jefferson Bezerra, nosso personagem



# Por que de Jefferson precisa de uma abordagem híbrida?



Executar cargas de  
trabalho localmente



Executar cargas de  
trabalho na nuvem

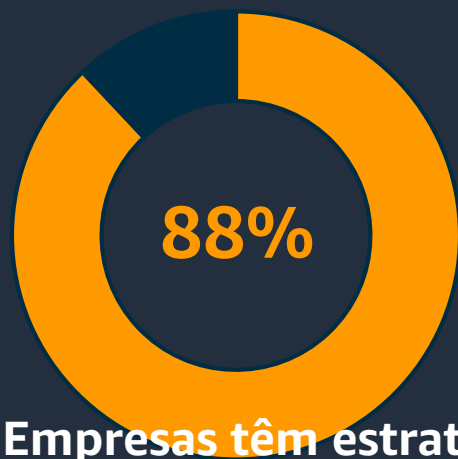


Integrar  
aplicações



Aproveitar  
habilidades e  
recursos

# Ainda é um mundo híbrido

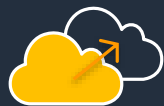


**Empresas têm estratégia em nuvem**



**Gastos em infraestrutura ainda no local**

# Casos de uso para uma abordagem híbrida



Cloud  
burst



Backup e disaster  
recovery



Migração e Modernização  
de Aplicativos





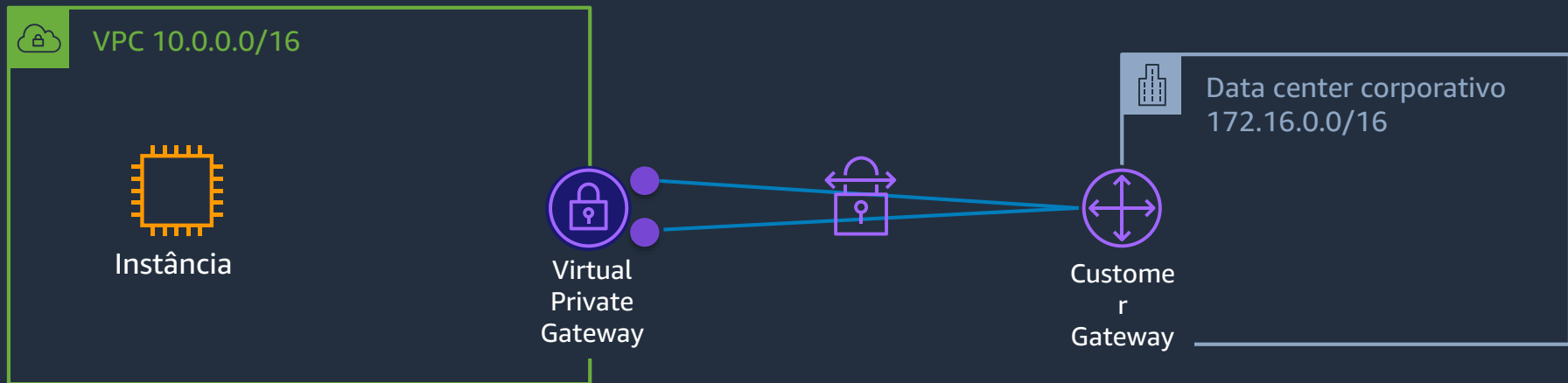
**Desafio 1: Como conectar o meu datacenter com a nuvem?**

# AWS VPN



VPN site to site da AWS

# VPN site to site na AWS

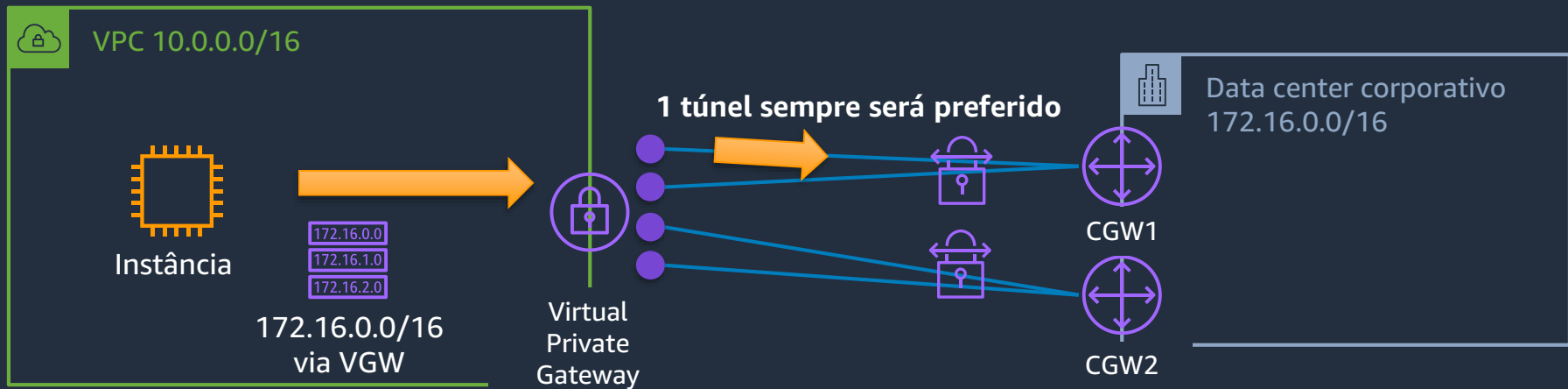


1x conexão VPN = 2x túneis VPN

1x túnel VPN = 1,25Gbps

# VPN site to site na AWS

## Roteamento estático ou dinâmico (BGP)

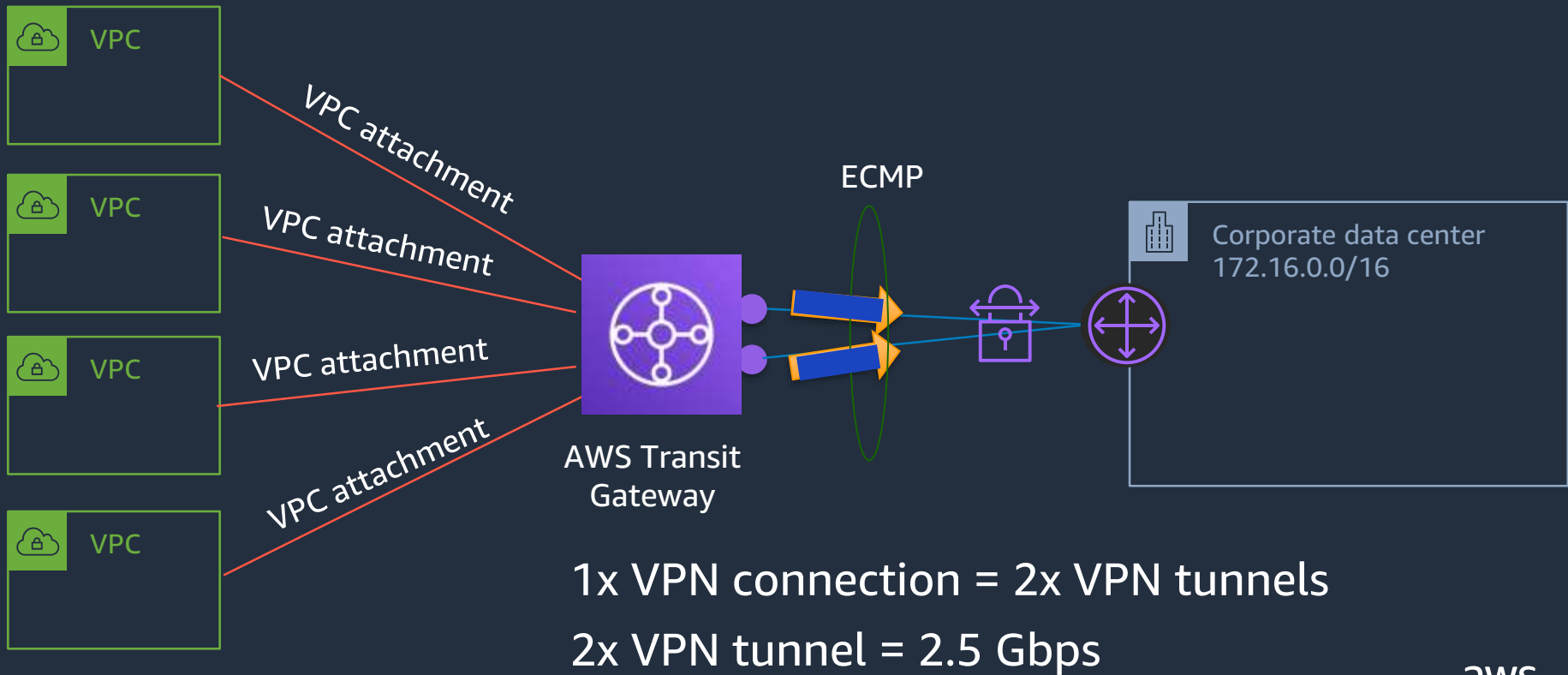


1x conexão VPN = 2x túneis VPN

1x túnel VPN = 1,25 Gbps



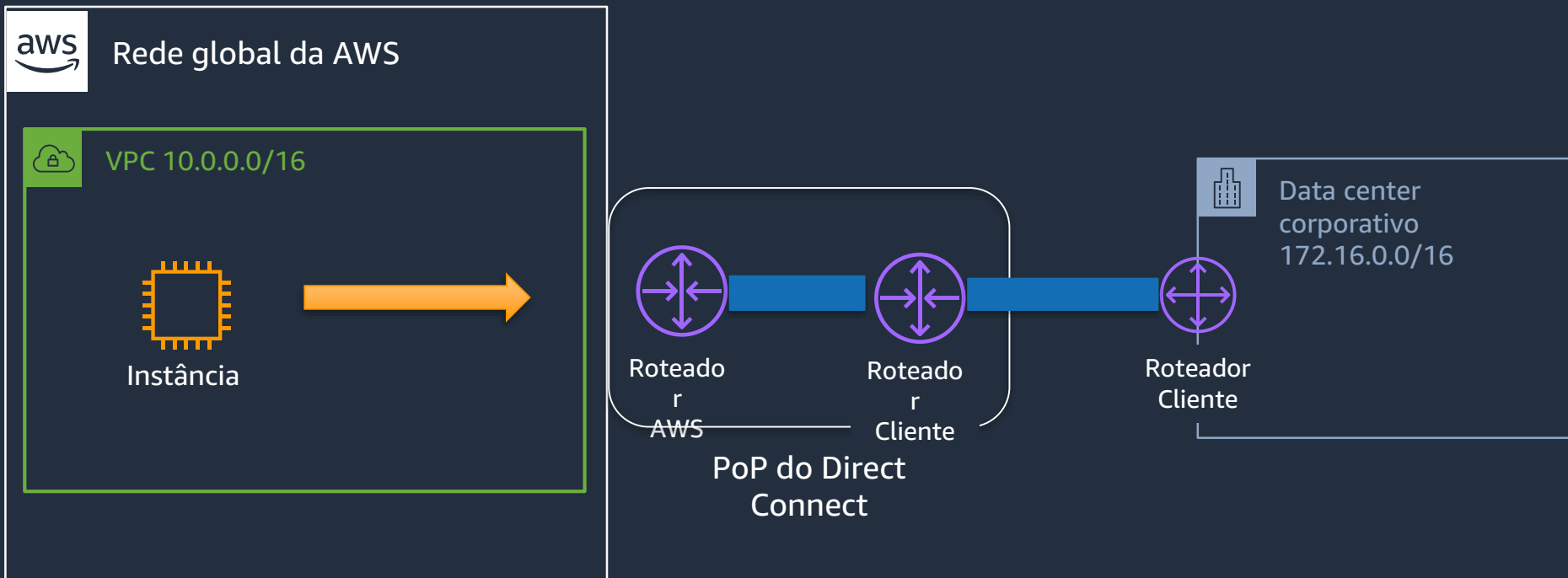
# VPN site to site na AWS (TGW + ECMP)



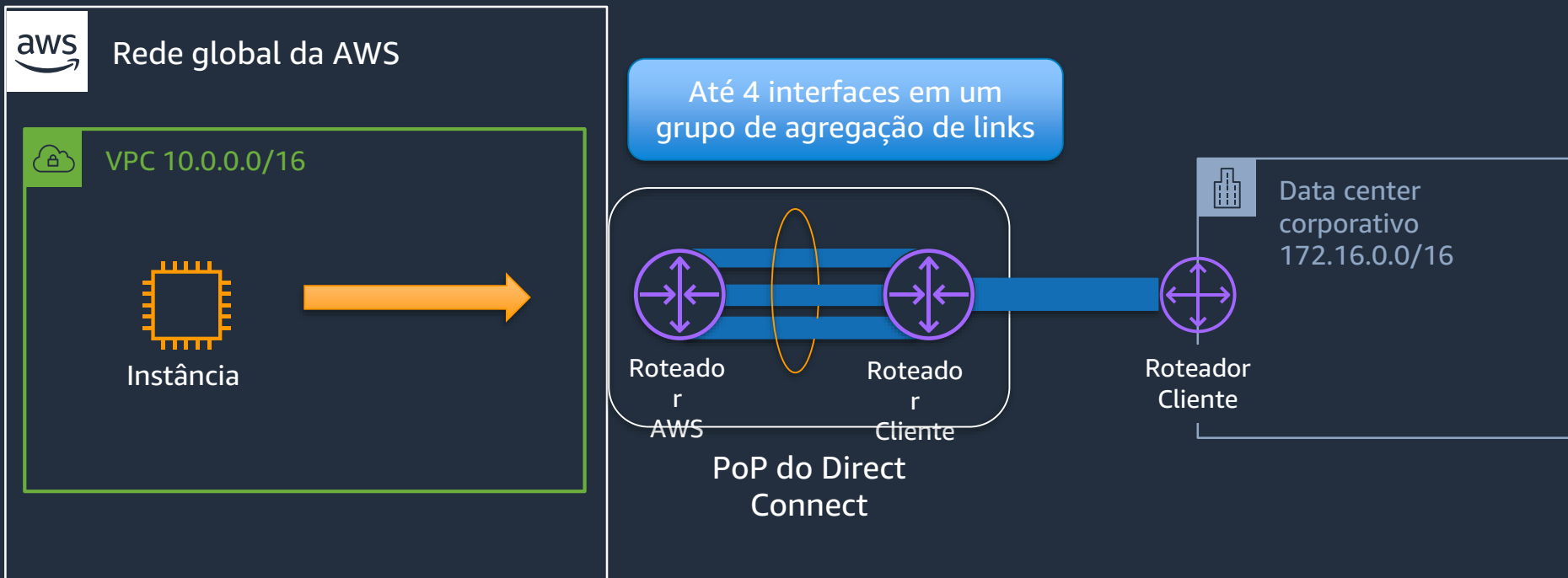
# AWS Direct Connect



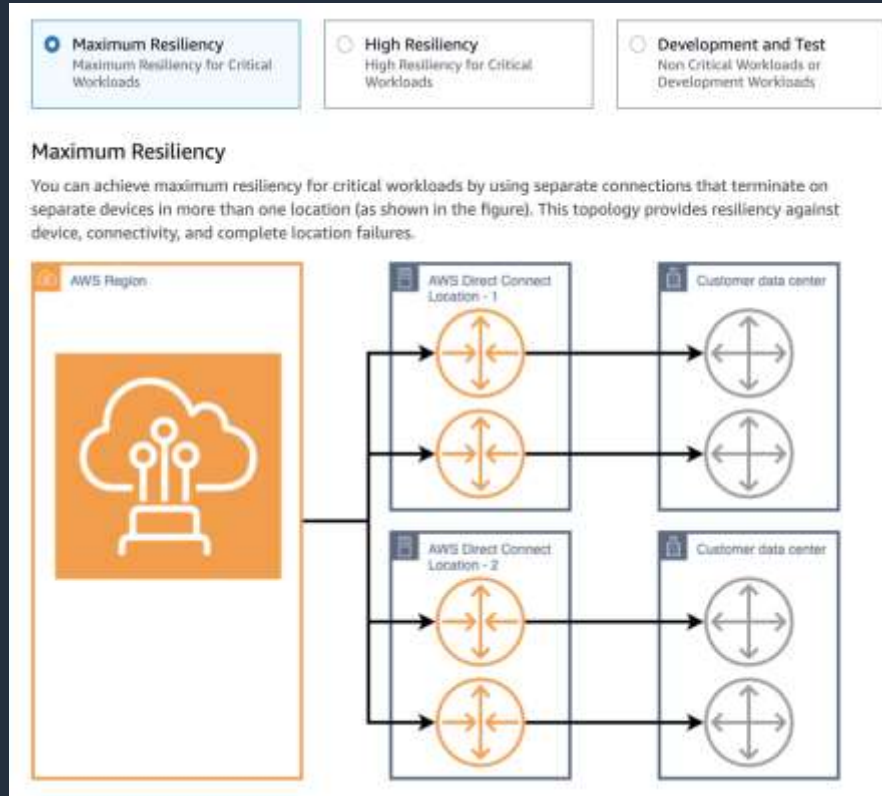
# AWS Direct Connect — Conexão física



# AWS Direct Connect — Agregação de links



# Ferramenta de configuração de resiliência



# AWS Direct Connect — Tipos de interface

- **VIF privado**— Usado para se conectar a Amazon VPCs usando endereços IP privados; diretamente ou via gateway Direct Connect
- **Trânsito VIF**— Usado para se conectar a gateways de trânsito via gateway Direct Connect
- **VIF público**— Usado para acessar todos os serviços públicos da AWS usando endereços IP públicos

**Todas as interfaces virtuais são VLANs 802.1Q com peering BGP**

# AWS Site-to-Site VPN ou AWS Direct Connect

	AWS Site-to-Site VPN	AWS Direct Connect
Media	Over the Internet	Physical, dedicated connection (not using Internet) = consistent performance, reduced bandwidth cost
Time to setup	Easy to install, setup in minutes	Some set-up time required – can be few days
Bandwidth	1 VPN tunnel = 1.25Gbps	1 Direct Connect Connection 50Mbps - 10Gbps
Encryption	Encrypted in transit	Not encrypted in transit
Cost	Charged per hour per VPN connection + Data Transfer	Charged per port hour + Data Transfer

# Desafio 2: Como tratar identidade e autenticação?





# Opção para implantação do AD

Self-managed,  
On-premises



Autogerenciado,  
Amazon EC2



Gerenciado  
pela AWS,  
Nuvem AWS



Gerenciado pela  
AWS  
↓  
Microsoft AD

# Apresentando o AWS Managed Active Directory



Migre facilmente suas cargas de trabalho dependentes de diretório, aproveitando um serviço gerenciado



Fornecer SSO e gerenciamento de acesso sem sincronizar dados de identidade



Use o Microsoft Active Directory integrado a outros serviços e aplicativos da AWS

# Principais recursos do AWS Managed Microsoft AD



**Microsoft AD real**



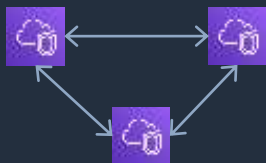
**Suporte a Trus**



**Suporte à política de grupo**



**ingresso no domínio de forma transparente**



**Suporte a várias contas e VPCs**



**Alta disponibilidade e backups diários**



**Infraestrutura gerenciada pela AWS**

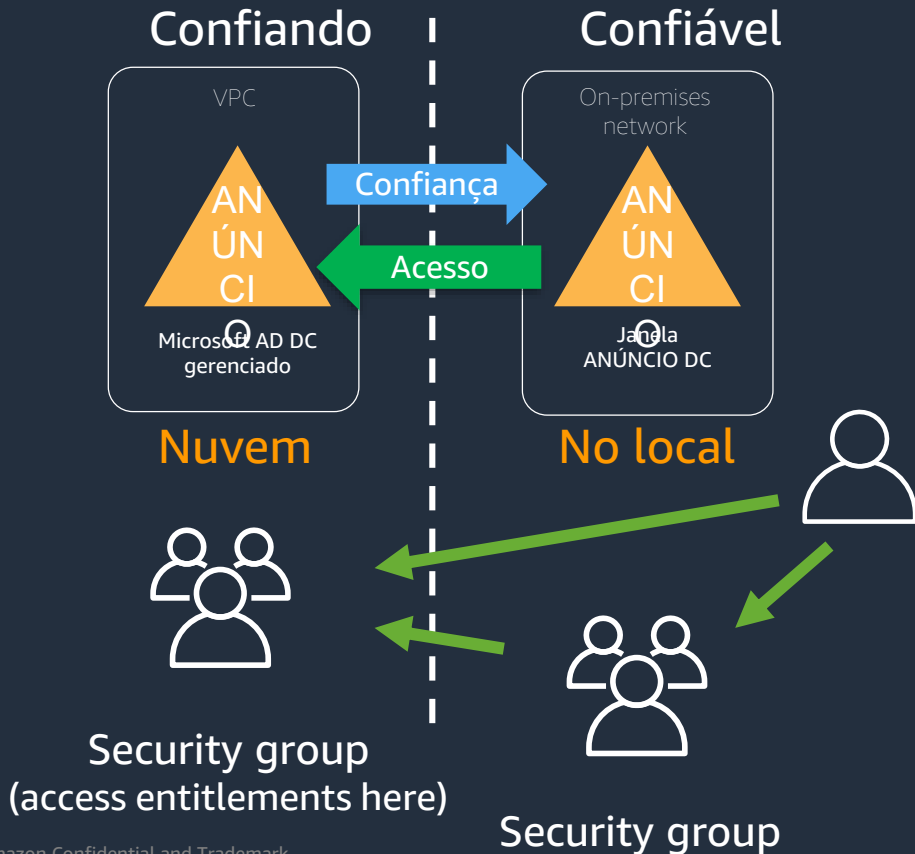
# Active Directory: modelo de confiança

# Entendendo o modelo de confiança



## Forest Trust

- Sem acesso por padrão
- Confiança usada para ler objetos no diretório



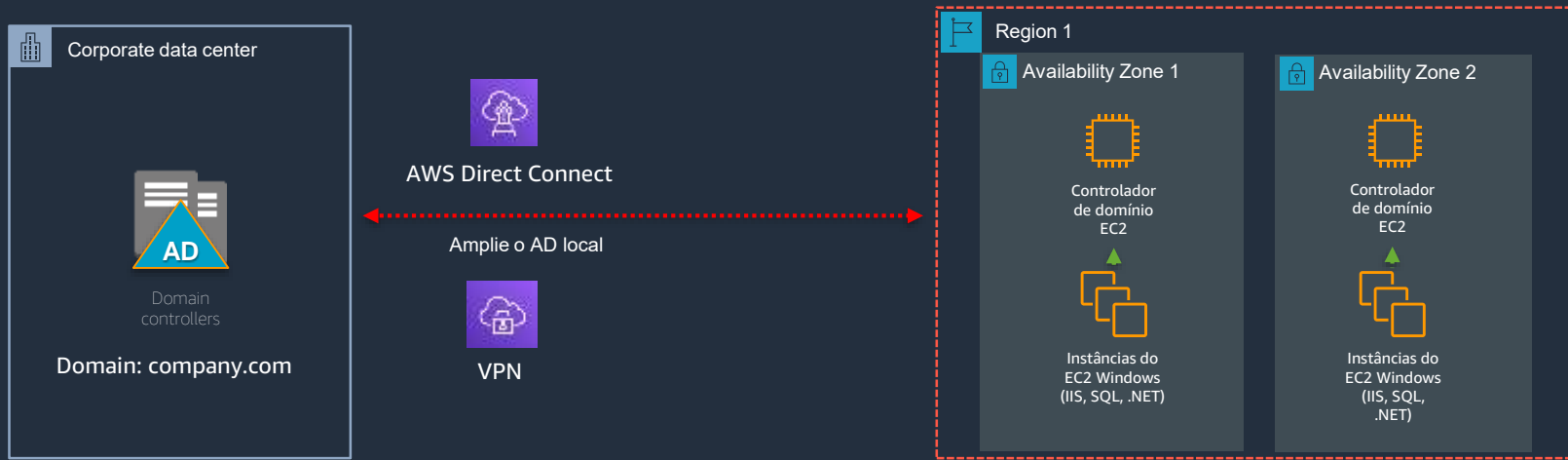
# Benefícios do modelo de confiança



- **Testado e comprovado pelo tempo** mecanismo de conectividade AD nativo.
- **Sem movimento ou transferência** de informações de identidade, mas capacidade de utilizá-las.
- **Menos requisitos de porta de rede** em comparação com as alternativas.
- **Bem documentado** fluxos de comunicação e configurações de segurança.

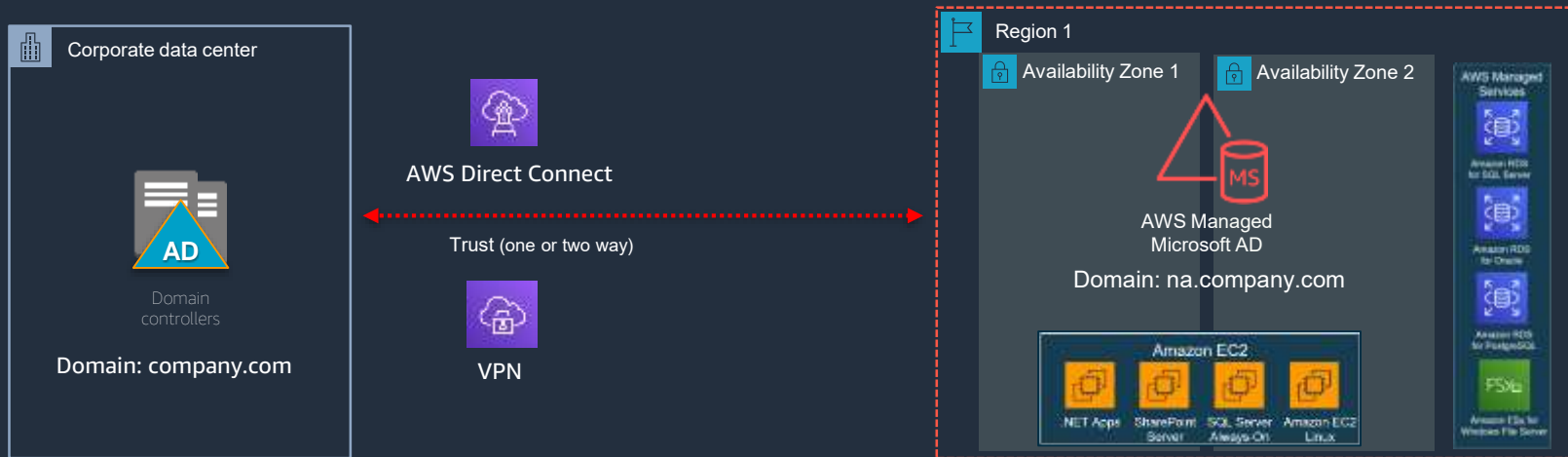
# Arquiteturas de referência

# Instâncias do EC2 para o AD local (design de região única)





# Domínio de recursos (design de região única)



# Considerações adicionais sobre design de rede



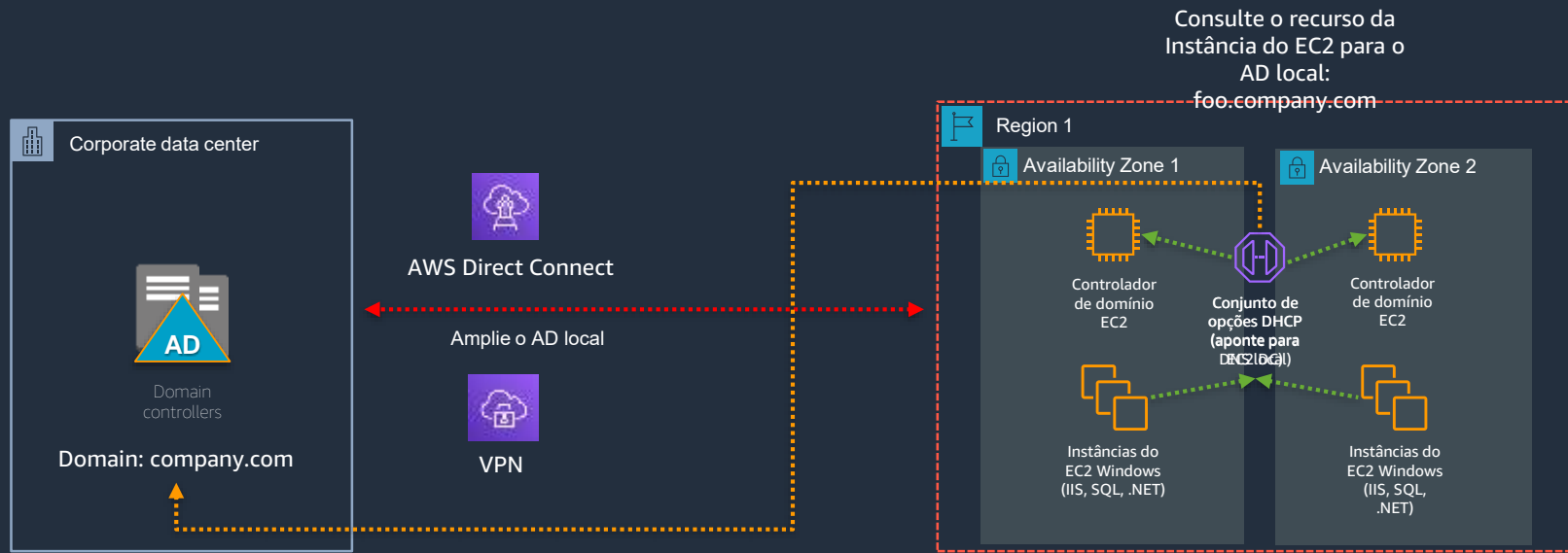
Amazon VPC



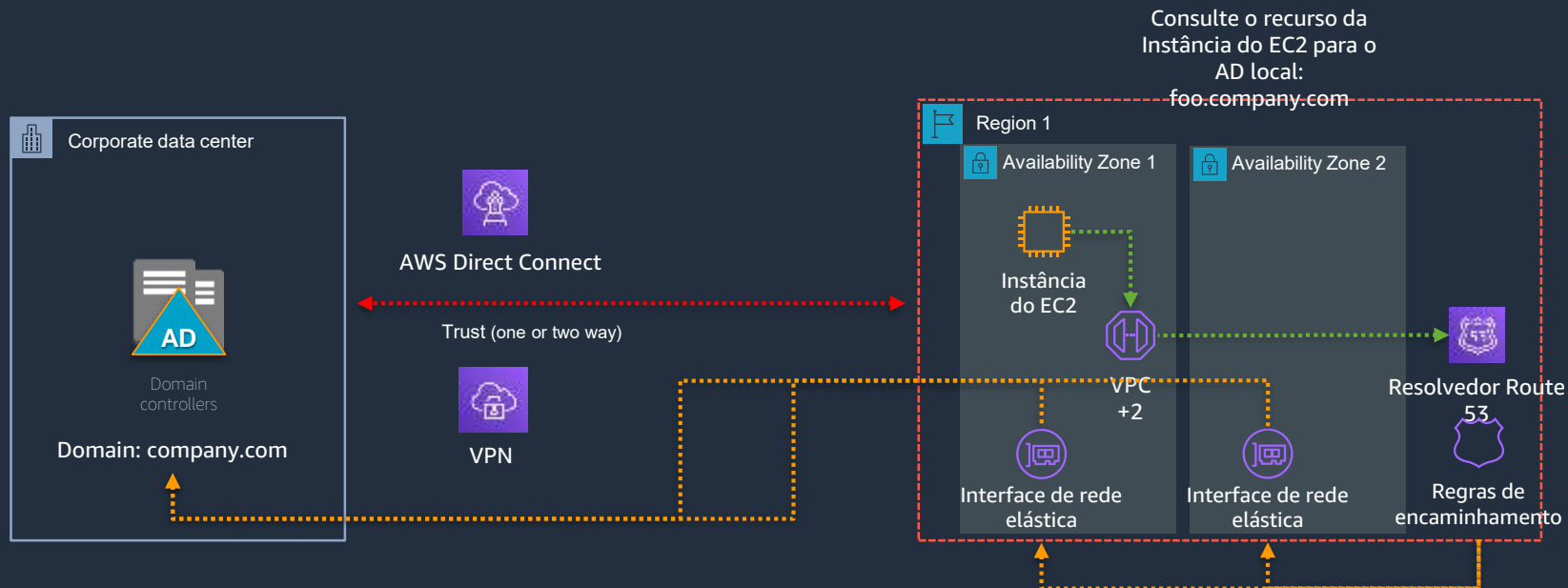
Amazon Route 53


- Conjunto de opções DHCP para o diretório, ou **AWS Managed Microsoft AD** no local atribua as opções de DHCP definidas à VPC atribuída ao Serviço de Diretório
  - Prós: permite que todas as instâncias nessa VPC apontem para o domínio especificado e os servidores DNS para resolver seus nomes de domínio. Isso evita a necessidade de configuração manual do DNS em instâncias do EC2, Windows ou Linux.
  - Contras: não pode ser compartilhado entre contas, exigindo que um conjunto de opções DHCP seja criado em contas adicionais.
- Crie endpoints de saída do Route 53 Resolver e encaminhe regras para **AWS Managed Microsoft AD** no local
  - Prós: deixe as opções de DHCP definidas como **DNS fornecido pela Amazon(+2)**, que é a configuração padrão, e as regras de encaminhamento podem ser compartilhadas com outras contas, tornando essa uma solução escalável. Isso é ideal para configurações de várias contas em que a centralização é desejável.
  - Contras: várias estratégias de design a serem consideradas e, dependendo da configuração, pode haver limites a serem superados.

# Exemplo de conjunto de opções DHCP



## Exemplo do Route 53 Resolver





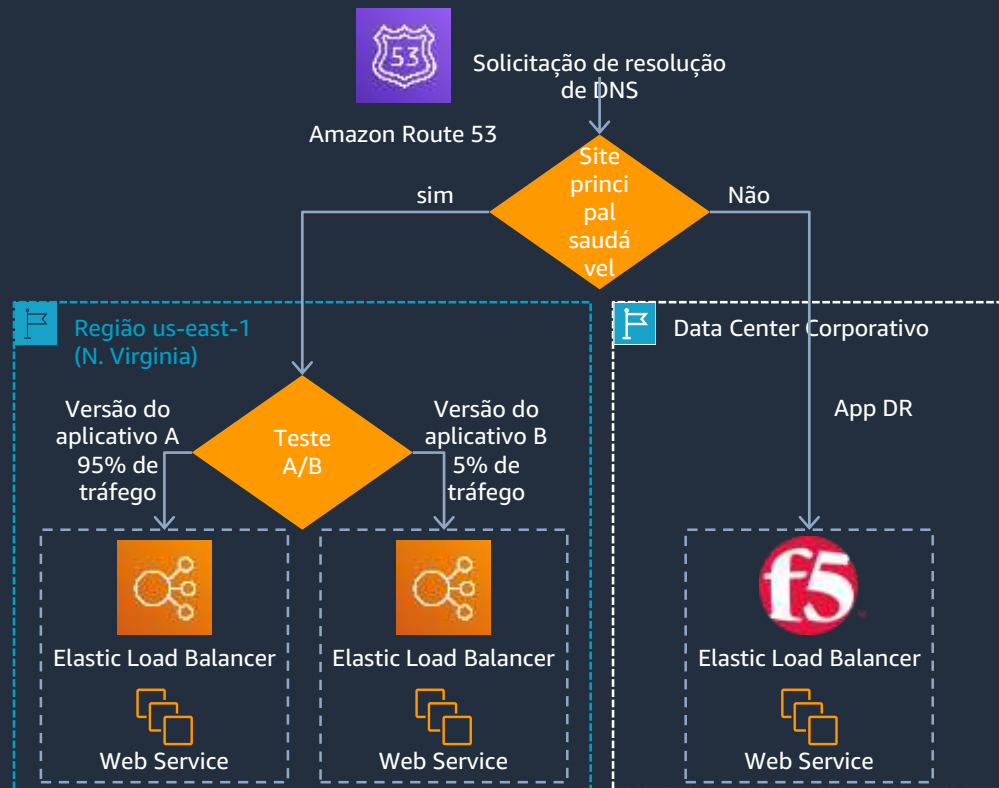
Desafio 3: Como distribuir  
tráfego entre o meu Data  
Center e a nuvem?



# DNS com o Amazon Route 53

# O que é o Amazon Route 53?

- Serviço AWS DNS
- Registro de domínio
- Resolução de nomes de domínio
- 100% de disponibilidade SLA
- Verificações de saúde
- Failover de DNS
- Roteamento baseado em latência
- Roteamento baseado em localização geográfica
- Round Robin ponderado
- DNS privado para VPC

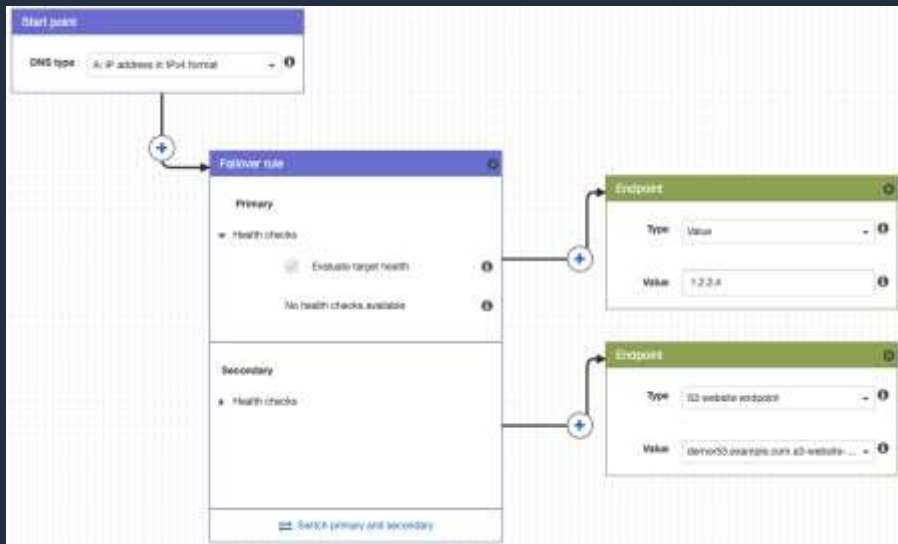


# Conceitos do Route 53: Políticas de roteamento

- As Políticas de Roteamento controlam como o Route 53 seleciona quais registros usar para responder a consultas.
  - Usado em conjunto com verificações de saúde para direcionar consultas para alvos saudáveis.
- Tipos de políticas:
  - Política de roteamento simples
  - Política de roteamento de failover
  - Política de roteamento de geolocalização
  - Política de roteamento por geoproximidade
  - Política de roteamento de latência
  - Política de roteamento de respostas multivaloradas
  - Política de roteamento ponderada



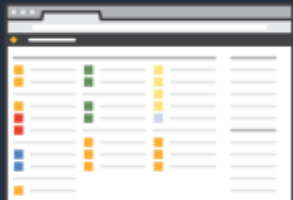
# Conceitos do Route 53: Fluxo de tráfego



- Defina fluxos poderosos que contenham muitas políticas.
- Versionado, implantado atomicamente.
- Use o construtor de fluxo visual ou JSON.
- O Route 53 gerencia a hierarquia subjacente de registros ALIAS, surgidos na zona hospedada como um único conjunto de registros.

# Entrega de conteúdo com o Amazon CloudFront

# Casos de uso de uma rede de entrega de conteúdo



Entrega em todo o site



Aceleração de API



Conteúdo personalizado  
usando Lambda @Edge



Entrega de objetos  
estáticos



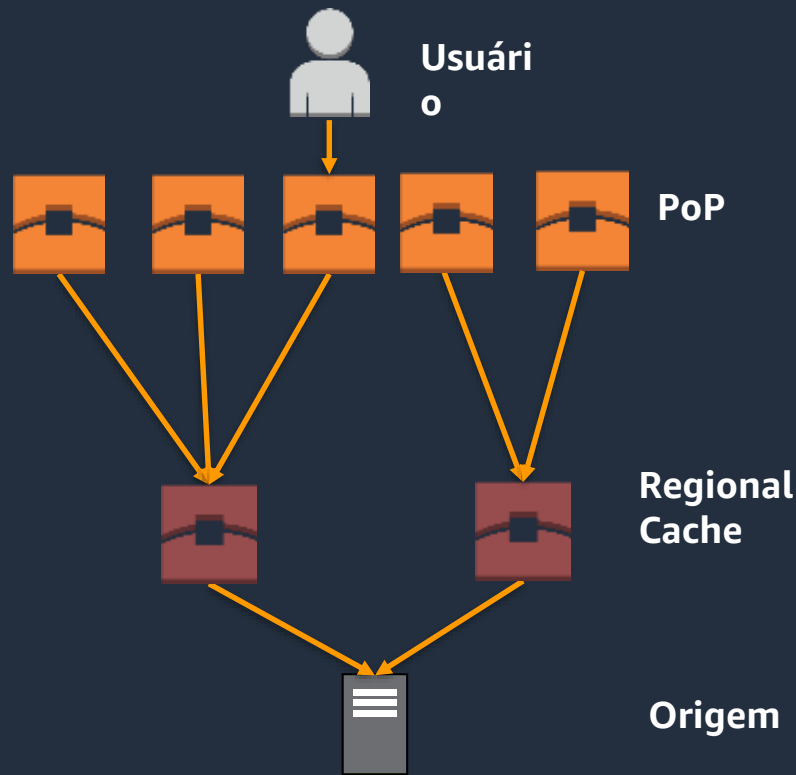
Streaming de vídeo



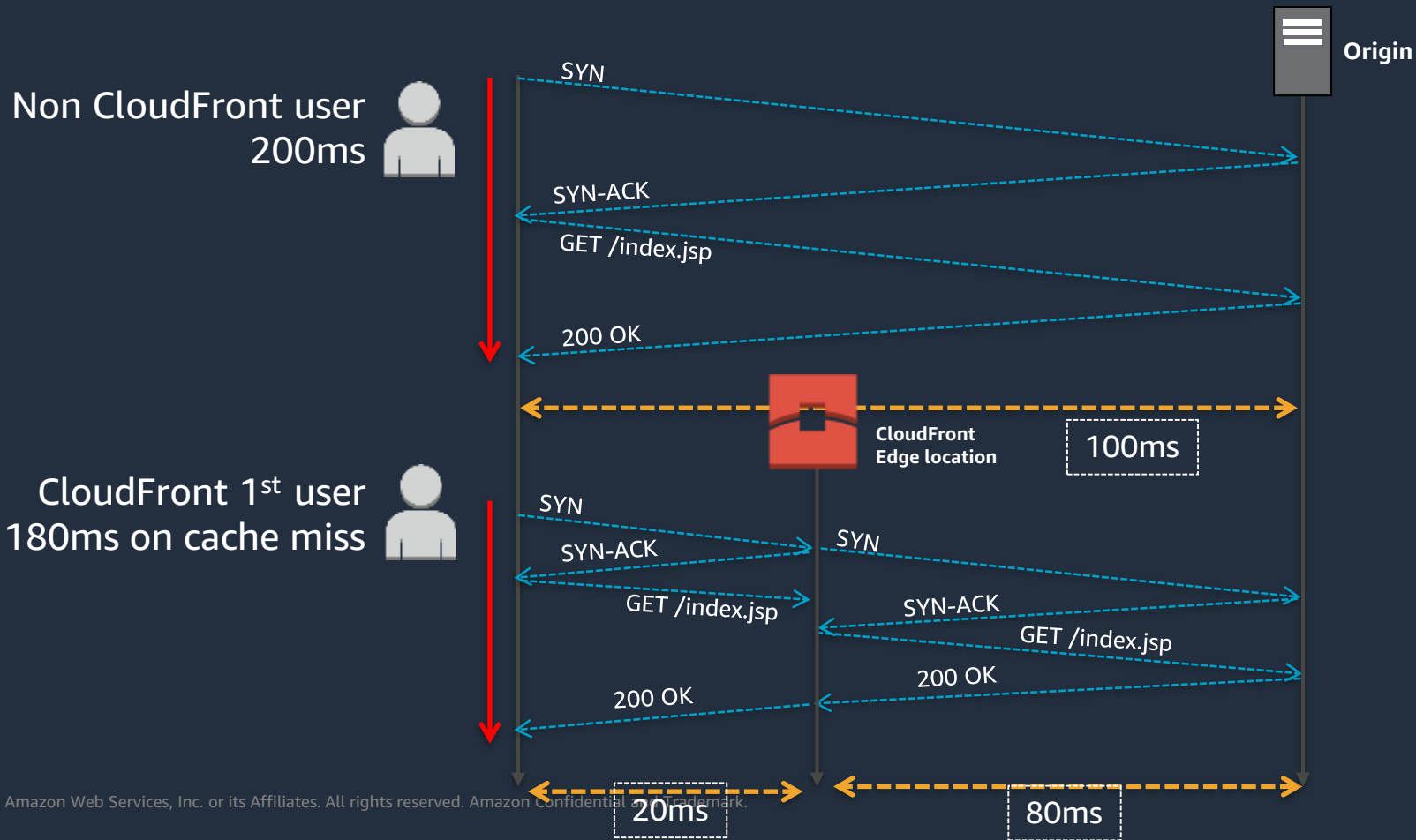
Downloads de arquivos  
grandes

# Arquitetura CloudFront

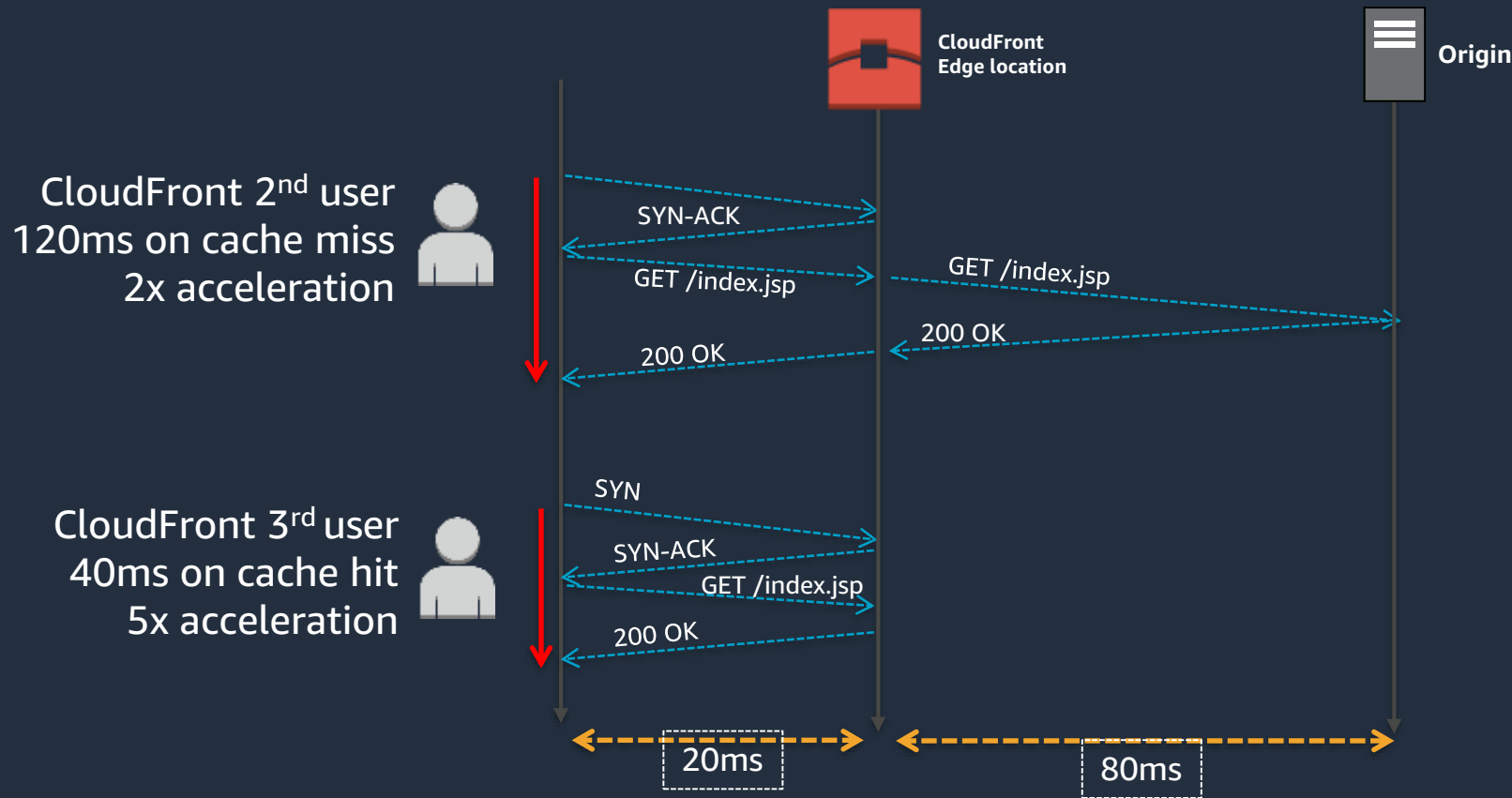
- Roteamento inteligente de DNS com base em latência e disponibilidade
- Os pontos de presença são baseados no SuperPoP modelo
- Serviço DNS Route53
- Armazenamento em cache
- Proteção contra DDoS
- WAF
- Controle de acesso com identidade de acesso Origin, URLs/cookies assinados e restrições geográficas.
- Caches de borda regionais
- PaisMidtierArmazenamento em cache
- Otimização de TCP
- Persistência de conexão de origem



# Aceleração de entrega (1/2)



# Aceleração de entrega (2/2)

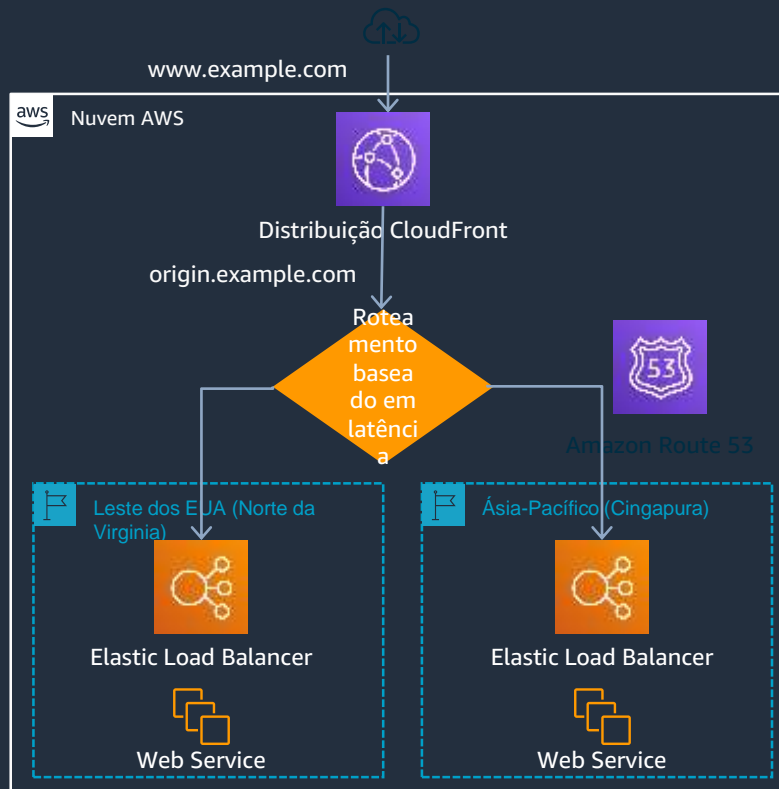


# Aproxime a computação dos usuários finais com Lambda @Edge

- Fornece capacidade de computação próxima aos usuários finais.
- Desenvolva código em Node.js ou Python
- O processamento pode ocorrer para todas as solicitações (lado do visualizador) ou apenas sem cache solicitações atendidas desde a origem (lado da origem)
- Casos de uso comuns incluem:
  - Teste A/B
  - Inserindo cabeçalhos HTTP adicionais
  - Reescrita e redirecionamento de URL
  - Inserção dinâmica de anúncios ou outra manipulação de respostas da origem.



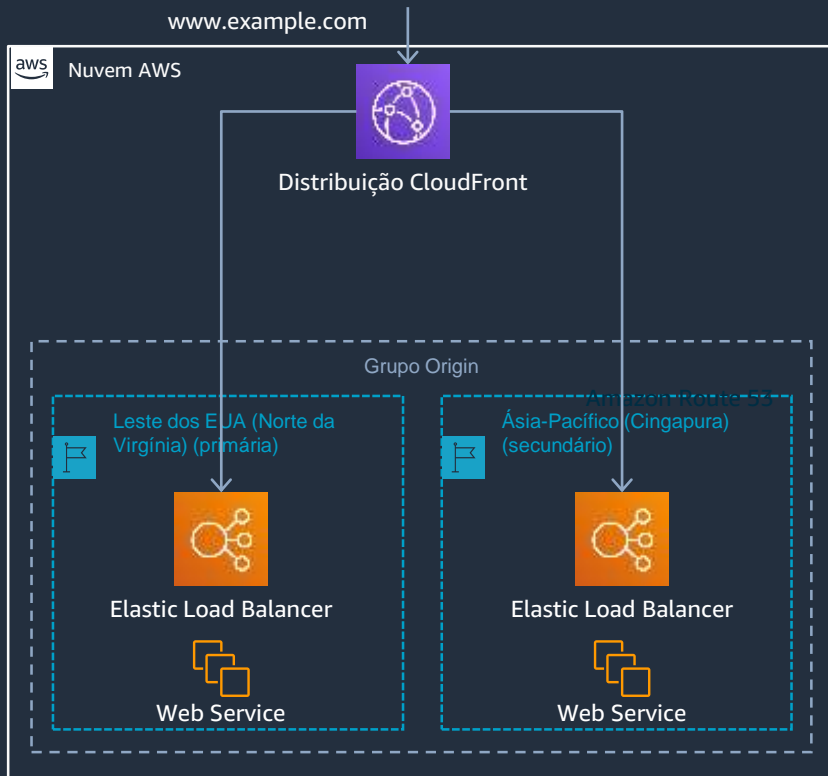
# Usar o CloudFront com o Route 53 para seleção Origin



- O CloudFront e o Route 53 podem ser usados juntos em aplicativos multirregionais.
- Configure a distribuição do CloudFront para uma origem personalizada.
  - A origem personalizada aponta para um conjunto de registros do Route 53.
  - Use o roteamento baseado em latência para enviar solicitações de origem para a região mais próxima do POP do CloudFront.
  - Use conjuntos de registros de failover e verificações de integridade para selecionar uma origem personalizada alternativa ou um bucket estático do S3 em caso de falha.



# Failover de origem do CloudFront



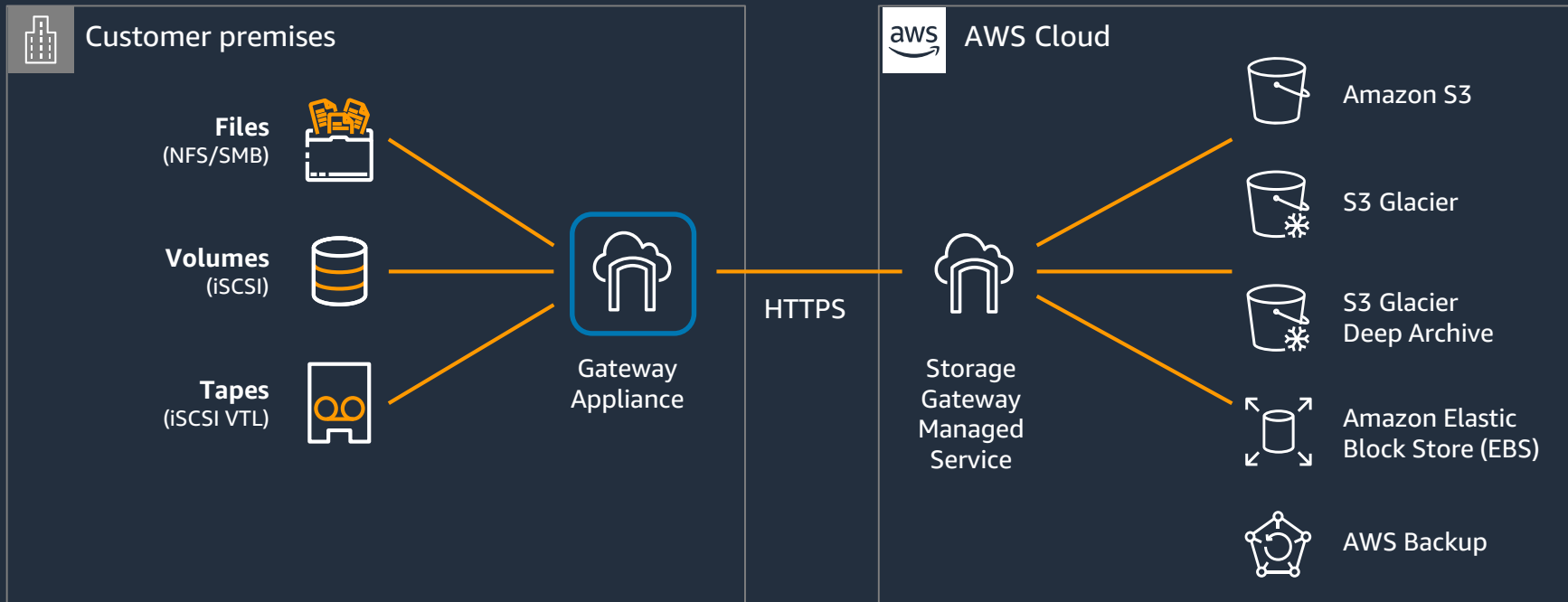
- Use para casos de failover simples.
- O CloudFront sempre tenta a origem primária primeiro.
- Usa origem secundária se o primário retornar resposta de erro ou o tempo de espera.
- Pode ser usado para fornecer failover entre origens do S3 em duas regiões.
  - Não é possível com o failover de origem baseado no Route 53 devido a requisitos exclusivos de nome de cabeçalho/bucket do host.

# Desafio 4: Como integrar o meu armazenamento local com a nuvem?



# AWS Storage Gateway

Acesso local a armazenamento em nuvem virtualmente ilimitado



Appliance Configuration: VMware, Hyper-V, EC2, Hardware

Integrated with IAM, KMS, CloudTrail,  
CloudWatch services

# File Gateway

Armazene e acesse objetos no Amazon S3 a partir de aplicativos baseados em arquivos com cache local



## Casos de uso

Faça backup de dados locais para a nuvem

Mude o armazenamento local para compartilhamentos de arquivos com suporte em nuvem

Acesso de baixa latência aos dados na AWS para aplicativos locais

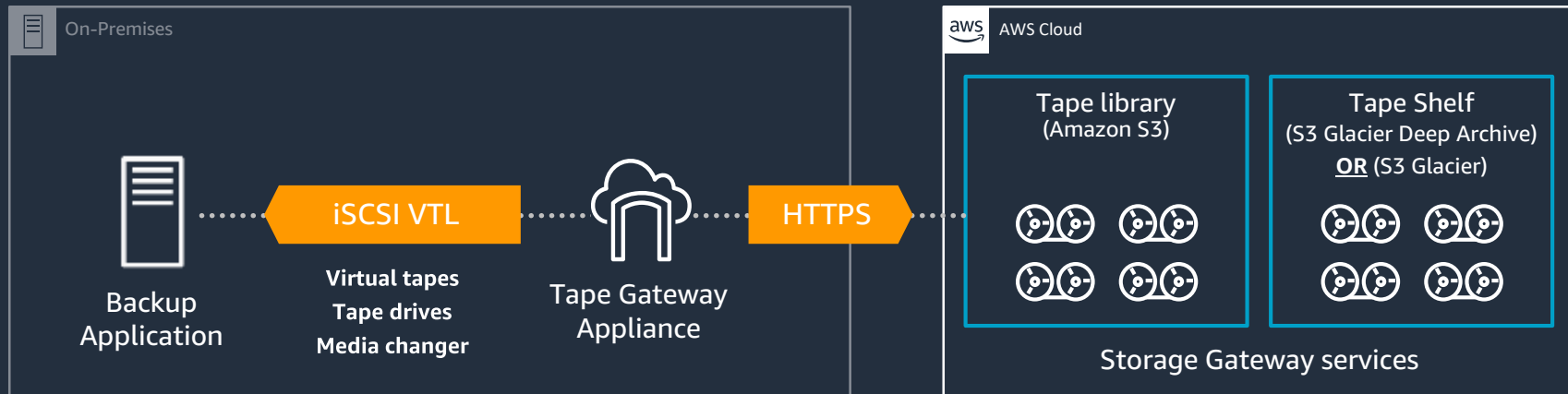
# Habilitar cargas de trabalho na nuvem



- Aplicativos baseados em NFS ou SMB gravam no S3 — um objeto por arquivo
- Utilize a capacidade praticamente ilimitada do S3
- Aproveite os recursos de computação habilitados para S3 em relação a conjuntos de dados armazenados NFS/SMB
- Ativar a funcionalidade Analytics e Machine Learning usando conjuntos de dados existentes

# gateway de fita

Apresentar fitas virtuais com suporte em nuvem para aplicativos de backup locais



## Benefits

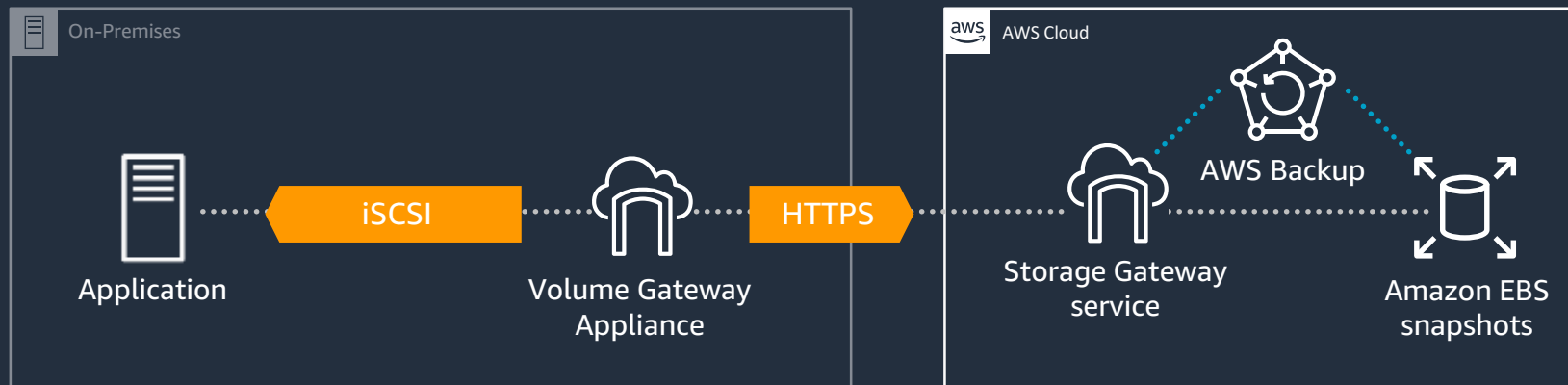
No changes to backup workflows

Supports all leading backup applications

Restores in hours

# Volume Gateway

Apresentar armazenamento em bloco no local apoiado por armazenamento em nuvem

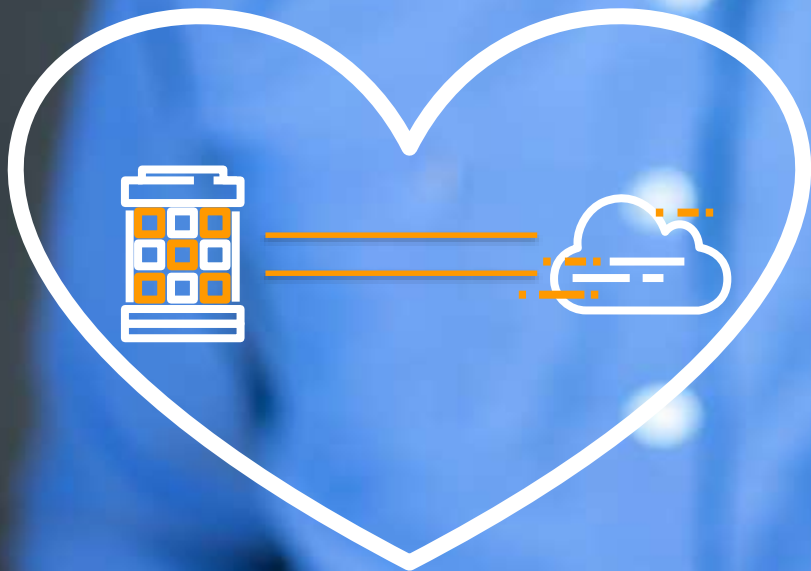


## Benefícios

Armazenamento em blocos com suporte em nuvem

Integrado com snapshots do EBS para facilitar a restauração na AWS

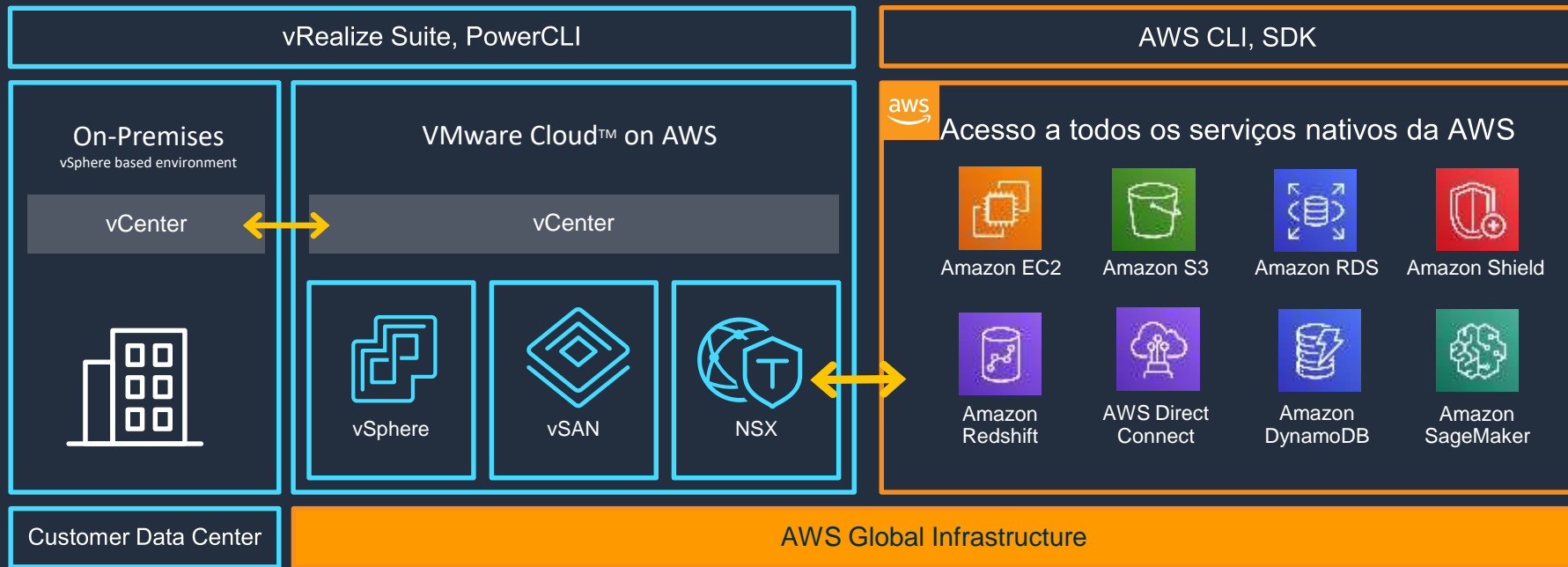
Integrado ao AWS Backup para gerenciar backups de volumes locais





# VMware Cloud on AWS

Inovação projetada conjuntamente pela VMware e AWS



# Benefícios do VMware Cloud no AWS



Gerenciado  
pela VMware



Consistência  
operacional



Portabilidade  
de carga de  
trabalho



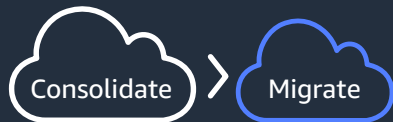
Integração  
nativa



Modernização de  
aplicativos

# Casos de uso orientados por atividade

## Cloud Migrations



Application specific

---

Data center wide

---

Infrastructure refresh

## Data Center Extension



Footprint expansion

---

On-demand capacity

---

Test/dev

## Disaster Recovery



Protect additional workloads

---

DR data center replacement

---

Add or modernize  
DR solutions

## Modernization



Application modernization

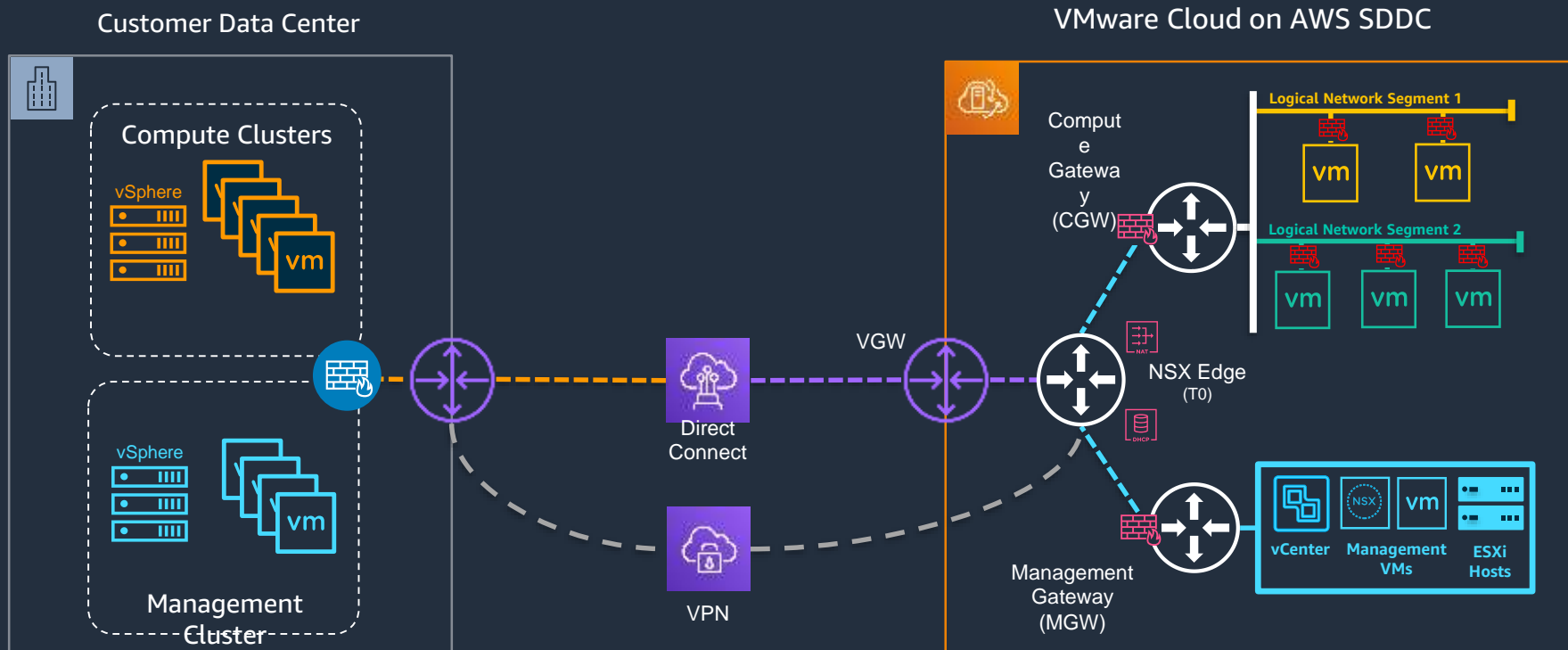
---

Next-gen app build out

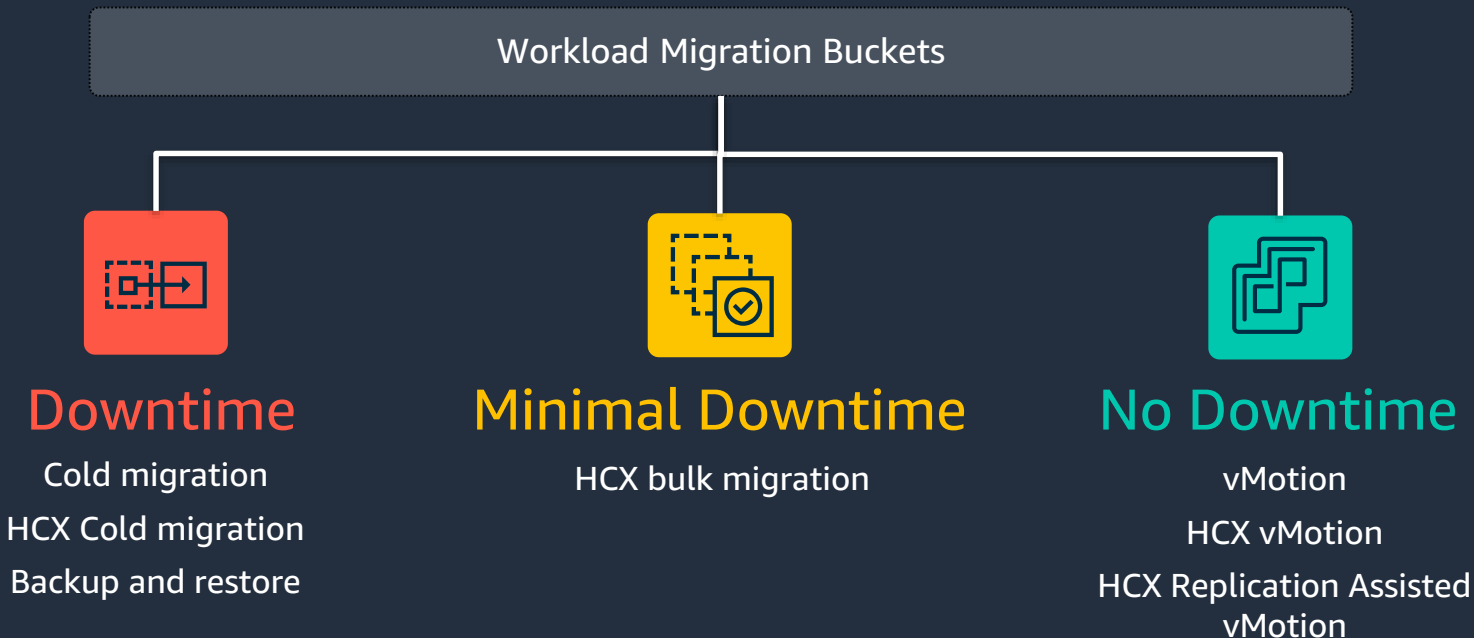
---

Enterprise workloads

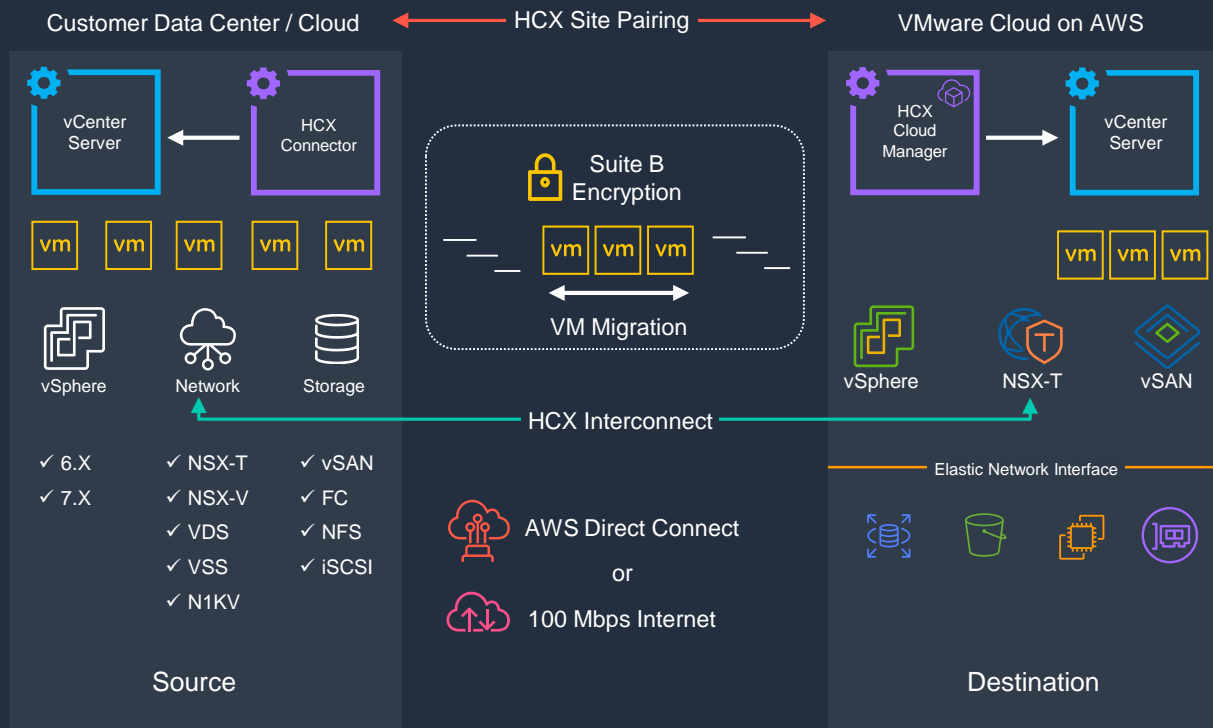
# Conectividade de locais para SDDC



# Opções de migração



# VMware Hybrid Cloud Extension™ (HCX) Service



Incluído com assinatura do VMware Cloud no AWS

Suporta vSphere 5.x, 6.x, 7.x (verificar interoperabilidade)

Migração de VM on-line e off-line em opções de escala

Agnóstico para design de rede vMotion on-prem

Otimização de WAN incorporada, de-dupe e compressão

Accessible via

- vSphere HTML5 plugin
- HCX standalone client
- HCX API & PowerCLI



Hora da Demo!



# Obrigado!

Karlos Correia — Arquiteto de Soluções

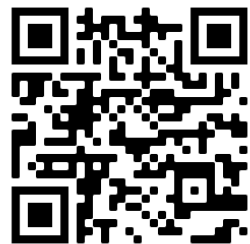
Kevin Lira — Arquiteto de soluções





# Agenda

- 12 de agosto - LGPD (Mariana Zonari e Fernando Gebara) - ok
- 26 de agosto - Ciência de dados (Jairo da Silva Junior) - ok
- 09 de setembro - DevOps – ok
- 23 de setembro - Estratégias de Migração para a nuvem - ok
- 07 de outubro - Modernização de backup - ok
- 21 de outubro – Experiencia do Usuário (UX) - ok
- 11 de novembro - Nuvem híbrida - ok
- 25 de novembro - **Containers**
- 08 de dezembro – Inteligencia Artificial e aprendizagem de máquina



<http://jornadasdigitais.cctd.ce.gov.br/>

# PREENCHA A AVALIAÇÃO!

- Ao final do webinar você vai receber um pedido de avaliação dos palestrantes, que será enviado amanhã no email de agradecimento.
- Dê o seu feedback para sabermos que você gostou e para podermos melhorar sempre!