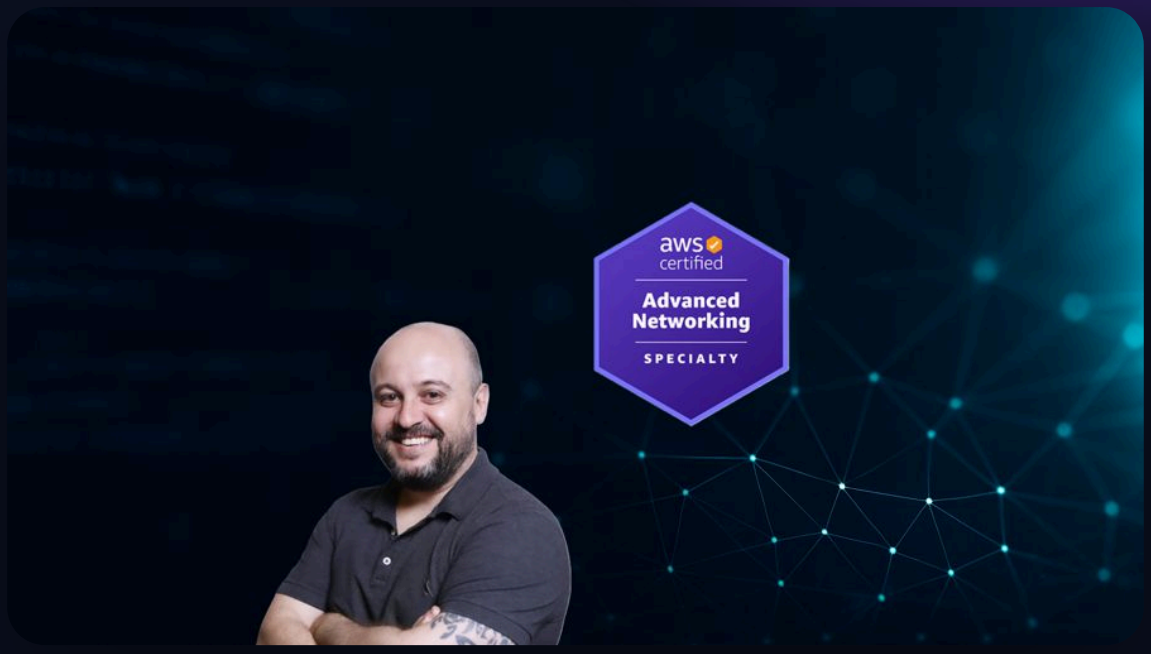


Guia de preparação ANS-C01

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

4
capítulos por domínio

28
questões comentadas

75%
nota de corte

6
provas completas no curso

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso ANS-C01: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 75%).

Mapa do exame

Cada prova do curso tem 65 questões e 170 minutos, no formato do exame. Referência de aprovação: 75%.

Domínio (capítulo)	Peso	Neste guia
1. Network Design	30%	18 conceitos · 14 pegadinhas
2. Network Implementation	26%	18 conceitos · 13 pegadinhas
3. Network Management and Operation	20%	18 conceitos · 13 pegadinhas
4. Network Security, Compliance, and Governance	24%	18 conceitos · 14 pegadinhas

> **Como ler os capítulos:** os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Network Design

Uma companhia de SaaS opera três VPCs em us-east-1: 'app-vpc', 'data-vpc' e 'shared-services-vpc'. A 'shared-services-vpc' hospeda ferramentas de monitoramento e bastion hosts que precisam acessar recursos nas outras duas VPCs. A empresa quer um design escalável para adicionar futuras VPCs em outras contas e regiões, com gerenciamento centralizado de rotas e menor complexidade operacional. Qual abordagem de conectividade atende melhor a esses requisitos?

A. Usar um Transit Gateway centralizado com as VPCs atuais e futuras, com o tráfego entre elas controlado pelas tabelas de rotas dele
B. Configurar uma VPC central de trânsito baseada em instâncias EC2 (appliance virtual) fazendo roteamento entre as VPCs por meio de múltiplas VPNs IPsec.
C. Criar emparelhamento (VPC peering) por completo malhado entre as VPCs e gerenciar as rotas à mão em cada tabela de rotas.
D. Ativar AWS PrivateLink entre as VPCs, expondo os serviços da 'shared-services-vpc' como endpoints privados.

D2 · Network Design

Uma empresa de varejo global está projetando uma nova arquitetura de rede na AWS para suportar três regiões (us-east-1, us-west-2 e eu-central-1). Os requisitos são: - Centralizar o controle de roteamento entre VPCs e conexões híbridas (VPN e Direct Connect). - Minimizar o número de túneis VPN entre regiões. - Permitir que algumas VPCs em diferentes regiões se comuniquem entre si, mas nem todas (não é full mesh obrigatório). - Suportar expansão futura para novas contas e regiões sem reconfigurar todos os túneis. Qual é o desenho de rede mais adequado para atender a esses requisitos?

A. Criar uma VPC central em us-east-1 e estabelecer peering VPC full mesh entre as VPCs nas três regiões. Encaminhar o tráfego on-premises através de uma instância NAT na VPC central.
B. Usar um Transit Gateway por região com peering entre eles, Direct Connect e VPN no de us-east-1 e rotas estáticas entre os Transit Gateways
C. Criar uma única VPC global com CIDR grande e sub-redes nas zonas de disponibilidade e regiões, utilizando rotas estáticas para conectar cada sub-rede ao ambiente on-premises via Direct Connect.
D. Utilizar AWS PrivateLink entre as VPCs e regiões para tráfego East-West e usar uma VPN site-to-site individual de cada VPC.

D3 · Network Design

Você está projetando uma arquitetura multi-região na AWS que precisa de comunicação privada, escalável e com gerenciamento centralizado de rotas entre diversas VPCs em diferentes regiões. A solução deve evitar o acoplamento direto entre VPCs e permitir segmentação de tráfego por domínio (por exemplo, produção e desenvolvimento) usando diferentes tabelas de rotas. Qual abordagem de design é mais adequada para atender a esses requisitos?

A. Centralizar as workloads em uma única VPC por região e usar Security Groups para controlar o tráfego entre domínios, sem utilizar Transit Gateway
B. Utilizar VPC peering entre as VPCs em diferentes regiões e aplicar listas de controle de acesso (ACLs de rede) para segmentar o tráfego entre domínios
C. Usar um Transit Gateway em cada região com peering entre eles e várias tabelas de rotas para segmentar os domínios de produção e desenvolvimento
D. Criar túneis VPN site-to-site entre as VPCs em diferentes regiões e usar tabelas de rotas de VPC para isolar o tráfego entre ambientes

D4 · Network Implementation

Uma empresa está migrando aplicações legadas que utilizam multicast para uma VPC na AWS. Essas aplicações precisam enviar e receber tráfego multicast apenas entre instâncias em sub-redes específicas, sem alcançar a internet ou outras VPCs. A empresa já utiliza gateways de trânsito (AWS Transit Gateway) para interconectar diversas VPCs em múltiplas contas. Qual abordagem atende melhor ao requisito de multicast, mantendo o isolamento adequado e simplificando a operação?

A. Criar um gateway de internet dedicado para multicast e usar regras específicas de rota e de segurança para garantir que o tráfego multicast permaneça só dentro da VPC, sem sair para a internet.
B. Configurar um Network Load Balancer em modo UDP para o endereço de multicast e associar as instâncias como targets.
C. Ativar multicast no Transit Gateway, criar um multicast domain associado só às sub-redes envolvidas e registrar as ENIs como fontes e membros
D. Utilizar AWS PrivateLink para publicar um endpoint de serviço multicast e permitir que só as sub-redes específicas criem endpoints de interface para receber o tráfego multicast.

D5 · Network Implementation

Um arquiteto de redes precisa implementar um mecanismo centralizado de resolução de nomes entre dezenas de contas AWS, garantindo: - Administração central do DNS entre contas - Suporte a consultas entre VPCs em múltiplas regiões - Possibilidade de auditoria e delegação controlada de permissões para times diferentes - Menor acoplamento possível entre as contas consumidoras e a conta de infraestrutura de rede Qual é a abordagem MAIS adequada e aderente às boas práticas da AWS para atender esses requisitos?

A. Criar uma VPC central com servidores DNS baseados em EC2 rodando BIND, configurar DHCP Option Sets nas VPCs apontando para esses servidores, e usar peering de VPC para interconectar as VPCs.
B. Usar uma conta central de DNS com endpoints do Route 53 Resolver e regras de encaminhamento compartilhadas pelo RAM e associadas às VPCs das várias regiões
C. Configurar uma AWS Managed Microsoft AD em uma conta central, habilitar encaminhamento condicional de DNS para as VPCs e contas, e utilizar VPN site-to-site entre as contas para transportar o tráfego DNS.
D. Criar zonas hospedadas privadas do Route 53 em cada conta e região, usando a mesma zona (ex.: corp.internal), e automatizar a criação de registros.

D6 · Network Implementation

Uma empresa precisa conectar centenas de VPCs em múltiplas contas AWS usando AWS Transit Gateway (TGW). Os requisitos incluem: (1) isolamento rígido entre ambientes de Produção e Não Produção; (2) possibilidade de aplicar políticas centralizadas de fluxo de tráfego (blackhole, rota padrão, inspeção em firewall central); (3) evitar sobrecarga operacional de atualização manual de rotas em larga escala; (4) garantir que certas VPCs somente possam falar com uma VPC de serviços compartilhados, nunca diretamente entre si. Qual abordagem de design atende melhor a esses requisitos?

A. Criar um único AWS Transit Gateway, anexar as VPCs ao mesmo domínio de roteamento e configurar rotas à mão em cada tabela de rotas de VPC para controlar o tráfego permitido
B. Criar um único AWS Transit Gateway e utilizar só uma tabela de rotas do TGW com propagação automática das rotas dos anexos, delegando o controle de tráfego só às ACLs de rede e grupos de segurança das VPCs
C. Criar VPC peering em malha completa entre as VPCs de Produção e usar um único AWS Transit Gateway só para as VPCs de Não Produção, aplicando políticas de segurança no TGW para isolar Produção de Não Produção
D. Usar dois Transit Gateways (Prod e Não Prod), cada um com tabelas de rotas por função (serviços compartilhados, firewall, spokes) e associação e propagação seletivas

D7 · Network Management and Operation

Uma equipe de operações de rede administra centenas de contas AWS em uma organização AWS Organizations com SCPs rígidos. Eles precisam garantir que todos os VPC Flow Logs de todas as VPCs (atuais e futuras) sejam: • Habilitados automaticamente em modo 'ALL' (accepted e rejected); • Centralizados em uma única conta de segurança; • Imutáveis, com proteção contra exclusão acidental; • Auditáveis, com controle de acesso baseado em princípio de menor privilégio. Qual combinação de ações atende melhor a esses requisitos com o menor esforço operacional contínuo?

A. Configurar AWS CloudTrail Organization Trail na conta de segurança, habilitar log de dados para VPC, e utilizar AWS Firewall Manager com políticas centralizadas para forçar a criação de Flow Logs em todas as VPCs, enviando-os para CloudWatch Logs na conta de segurança com KMS gerenciado pela AWS.
B. Criar um Transit Gateway central, anexar todas as VPCs a ele e habilitar VPC Flow Logs somente no Transit Gateway. Enviar os logs para uma conta de segurança via Amazon Data Firehose para um bucket S3 com criptografia SSE-S3, e usar políticas IAM para impedir exclusão de logs.
C. Usar um bucket S3 com Object Lock na conta de segurança, SCPs negando a exclusão de flow logs e buckets, e StackSets criando os flow logs em todas as contas
D. Criar um AWS Config Aggregator na conta de segurança, habilitar a regra gerenciada 'vpc-flow-logs-enabled' em todas as contas e usar AWS Lambda acionada por AWS Config para criar/atualizar Flow Logs em cada VPC, enviando-os para um bucket S3 na mesma conta. Usar políticas de bucket S3 e bloqueio de versão padrão para evitar exclusões.

D8 · Network Management and Operation

Um time de operações precisa implementar um processo centralizado de detecção e resposta a incidentes de rede em dezenas de VPCs distribuídas em múltiplas contas AWS. Os requisitos incluem: (1) visualização centralizada de tráfego suspeito entre VPCs e para a Internet; (2) possibilidade de automatizar respostas (como isolamento de instâncias via Security Groups) usando AWS Systems Manager Automation ou AWS Lambda; (3) redução do overhead operacional de gerenciar agentes em cada instância. Qual abordagem atende melhor a esses requisitos?

A. Criar um AWS Network Firewall em cada VPC, enviar logs para um Amazon S3 central, e usar consultas ad-hoc em Amazon Athena para acionar scripts manuais quando um padrão de tráfego suspeito for identificado.
B. Usar VPC Flow Logs em um CloudWatch Logs central, com metric filters e alarmes que acionam o Systems Manager Automation ou o Lambda para respostas automáticas
C. Instalar agentes de terceiros nas instâncias EC2 para enviar logs de rede para um SIEM externo e executar scripts de remediação remota.
D. Configurar AWS CloudTrail para registrar as chamadas de API de rede e usar AWS Config para acionar remediações automáticas baseadas em alterações de configuração, sem coletar dados de fluxo de tráfego.

D9 · Network Management and Operation

Uma empresa opera dezenas de VPCs em múltiplas contas AWS, interligadas por AWS Transit Gateway. O time de operação relata dificuldade em identificar rapidamente o caminho de rede percorrido por tráfego entre duas ENIs específicas (origem e destino) durante incidentes intermitentes de conectividade. Eles querem uma solução que permita rastrear o fluxo fim a fim, incluindo saltos em Transit Gateway e ENIs intermediárias, com o mínimo de impacto operacional e sem necessidade de instalar agentes em instâncias. Qual abordagem atende melhor a esses requisitos?

A. Usar o Reachability Analyzer entre as ENIs de origem e destino, com análises entre contas habilitadas pela integração com o Organizations
B. Habilitar VPC Flow Logs nas VPCs, exportar para Amazon CloudWatch Logs e usar Insights para consultar o caminho de rede hop-by-hop entre ENIs
C. Ativar AWS CloudTrail para as contas e utilizar os eventos de plano de controle para reconstruir o caminho de dados entre as ENIs
D. Habilitar AWS Network Firewall nas VPCs e usar os logs de tráfego do firewall para mapear o caminho completo entre origem e destino

D10 · Network Security, Compliance, and Governance

Uma empresa tem conexões Direct Connect dedicadas de 100 Gbps e precisa criptografar o tráfego no enlace entre o seu roteador e o dispositivo da AWS, sem perder desempenho com túneis IPsec. O que configurar?

A. MACsec na conexão dedicada, associando a chave CKN/CAK à conexão e configurando o roteador
B. Criptografia TLS no transit VIF, habilitada na configuração do Direct Connect gateway
C. Uma VPN Site-to-Site pública pela internet como caminho principal no lugar do Direct Connect
D. Um AWS Network Firewall na VPC para criptografar o tráfego que chega pelo Direct Connect

D11 · Network Security, Compliance, and Governance

Você está projetando um ambiente multi-conta na AWS com forte governança de segurança de rede. O time de segurança quer aplicar regras padronizadas de grupos de segurança em todas as contas de produção, garantindo que desvios sejam automaticamente detectados e corrigidos, além de manter visibilidade centralizada e trilha de auditoria das alterações. Qual serviço da AWS é MAIS apropriado para implementar essa padronização de grupos de segurança em escala, com gerenciamento centralizado e integração com AWS Organizations?

A. AWS Firewall Manager
B. AWS Control Tower
C. AWS Security Hub
D. AWS Config

D12 · Network Security, Compliance, and Governance

Você é responsável pela governança de rede em um ambiente multi-conta na AWS que utiliza AWS Organizations. A área de segurança determinou que: • Nenhuma VPC em nenhuma conta pode ter Internet Gateway anexado. • As contas de desenvolvimento não podem criar nem modificar regras de Security Groups. • Todas as VPCs devem permitir inspeção centralizada de tráfego via AWS Network Firewall em uma conta dedicada de segurança. Qual combinação de ações atende de forma mais eficaz a esses requisitos com o menor esforço operacional contínuo?

A. Usar uma SCP negando a criação e a anexação de internet gateways, políticas de security groups do Firewall Manager e Network Firewall centralizado nas VPCs
B. Criar políticas IAM em cada conta negando a criação de Internet Gateway e alterações de Security Groups, delegar uma conta administradora do AWS Firewall Manager para gerenciar políticas de AWS Network Firewall, mas sem utilizar Service Control Policies em AWS Organizations.
C. Configurar AWS Control Tower para as contas, usar Service Control Policies só para negar 'ec2:AuthorizeSecurityGroupIngress' em contas de desenvolvimento e configurar AWS WAF em Application Load Balancers para atuar como camada de inspeção centralizada de tráfego.
D. Criar NACLs padrão bloqueando todo tráfego de saída nas VPCs, utilizar AWS Config para detectar Internet Gateways e Security Groups não conformes e executar remediação automática via Systems Manager Automation, sem uso de AWS Firewall Manager.

01

CAPÍTULO 1 · 30% DA PROVA

Network Design

Design é o maior domínio e cobra o porquê de cada peça da arquitetura: Transit Gateway como hub regional, Cloud WAN como WAN global por política, VPC peering para poucos pares, PrivateLink e VPC Lattice para expor serviços, e Direct Connect com Direct Connect gateway para o híbrido. A prova descreve um cenário com muitas VPCs, várias contas e regiões e pede o desenho mais escalável e com menos operação; quase sempre peering em malha, VPN entre VPCs e roteador em EC2 são distratores. Também caem detalhes finos: allowed prefixes do DX gateway, resiliência máxima do Direct Connect, CIDRs sobrepostos, IPv6 com NAT64, endpoints centralizados e borda (CloudFront x Global Accelerator). Meu ponto fraco é perceber quando a solução mais simples (peering) é a certa porque o cenário tem só duas VPCs.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

AWS Transit Gateway

Hub regional que conecta VPCs, VPNs e Direct Connect com roteamento transitivo controlado por tabelas de rotas. A associação define qual tabela o attachment consulta; a propagação define quem aparece em cada tabela. Para várias contas, compartilhe pelo AWS RAM; o attachment é criado pela conta dona da VPC.

Segmentação com tabelas do Transit Gateway

Tabelas separadas por ambiente ou domínio (produção, desenvolvimento, terceiros) com propagação seletiva, por exemplo só a VPC de serviços compartilhados propagada nas tabelas de prod e dev. Uma única tabela com propagação de tudo cria conectividade total e empurra o isolamento para NACLs.

Peering entre Transit Gateways

Liga Transit Gateways de regiões diferentes com tráfego pela rede global da AWS e criptografia automática. Não usa BGP e não suporta propagação: os CIDRs remotos entram por rotas estáticas nos dois lados. O padrão multi-região é um Transit Gateway por região com peering entre eles.

AWS Cloud WAN

WAN global gerenciada definida por uma core network policy com segmentos (produção, desenvolvimento, parceiros) e regras de anexação e compartilhamento de rotas, sem configurar peering região a região. Service insertion usa um network function group com send-via (leste-oeste) e send-to (saída para a internet).

VPC peering

Conexão direta entre duas VPCs, sem custo de processamento por GB como o Transit Gateway e com menor latência, ideal para poucas VPCs com muito tráfego. Não é transitivo, não funciona com CIDRs sobrepostos e em malha completa cresce em N*(N-1)/2 conexões. Também não permite usar o NAT ou o gateway de outra VPC.

Direct Connect gateway e allowed prefixes

O Direct Connect gateway liga conexões Direct Connect a VGWs ou Transit Gateways de várias regiões, mas não roteia tráfego entre VPCs. Com Transit Gateway, o que o on-premises aprende vem da lista de allowed prefixes da associação DXGW-TGW, que aceita resumos como um /16.

Tipos de VIF

Transit VIF liga o Direct Connect gateway a Transit Gateways; private VIF liga a virtual private gateways (direto ou via Direct Connect gateway); public VIF alcança serviços públicos da AWS. Private VIF não se conecta diretamente a um serviço como o S3.

Resiliência do Direct Connect

O nível máximo recomendado sobrevive à falha de um dispositivo, de uma conexão e de uma localização inteira: conexões dedicadas em dispositivos separados em pelo menos duas localizações distintas, de preferência com roteadores on-premises redundantes e BGP. LAG em uma única localização não sobrevive à perda dela.

AWS Global Accelerator

Dá IPs estáticos globais anycast, entrada pela borda mais próxima e failover rápido entre regiões por health checks e pesos, para TCP e UDP. Endpoints podem ser NLBs ou ALBs regionais. Diferente do failover por DNS, não depende do cache de DNS dos clientes.

Amazon CloudFront e VPC origins

CloudFront é a camada de borda para conteúdo HTTP/HTTPS, com cache, TLS e Web ACL do WAF associada à distribuição. VPC origins permite usar um ALB interno em sub-redes privadas como origem, sem IP público. A prefix list gerenciada do CloudFront só restringe uma origem que continua pública.

Egress centralizado

VPC de egress com NAT gateways em duas AZs; a rota padrão das spokes aponta para o Transit Gateway e dele para essa VPC. Reduz custo fixo de NAT em cada VPC e centraliza o controle; a mesma VPC pode receber o firewall para inspecionar a saída. Compare o custo de processamento do Transit Gateway com a economia.

CIDRs sobrepostos

Para tráfego iniciado por um lado, adicione um CIDR secundário roteável com NAT gateway privado e roteie pelo Transit Gateway. Para expor só um serviço a muitos clientes com os mesmos CIDRs, use PrivateLink. Peering e Transit Gateway exigem CIDRs sem sobreposição.

Amazon VPC Lattice

Conectividade de aplicação entre serviços em várias VPCs e contas, com auth policies do IAM por serviço e suporte a CIDRs sobrepostos, sem gerenciar roteamento. A service network é compartilhada pelo AWS RAM. Não conecta redes inteiras nem escritórios.

AWS PrivateLink

Publica um serviço atrás de um NLB como endpoint service; cada consumidor cria um interface endpoint na própria VPC, com acesso privado iniciado só pelo cliente e isolamento entre consumidores. Para consumir de outra região, o provedor habilita a região como suportada e o cliente cria o endpoint localmente.

Amazon VPC IPAM

Planeja e aloca CIDRs de forma central, integrado ao Organizations, com pools por região e ambiente que entregam um bloco livre a cada nova VPC. Prefix lists agrupam CIDRs para regras e rotas, mas não alocam nem evitam sobreposição.

IPv6-only com DNS64 e NAT64

Para instâncias em sub-redes somente IPv6 acessarem destinos só IPv4, ative DNS64 na sub-rede e roteie o prefixo 64:ff9b::/96 para um NAT gateway público, que faz o NAT64. O egress-only internet gateway só encaminha IPv6.

VPC endpoints centralizados

Crie os interface endpoints numa VPC compartilhada sem DNS privado e associe às spokes private hosted zones com os nomes dos serviços; o DNS privado do endpoint só vale na VPC onde foi criado. Gateway endpoints existem só para S3 e DynamoDB e só atendem tráfego de dentro da VPC; do on-premises, use interface endpoint do S3.

Transit Gateway Connect, multicast e SiteLink

Connect attachment integra appliances SD-WAN ao Transit Gateway com GRE e BGP, sem IPsec e com mais banda que um túnel VPN. Multicast entre instâncias de várias VPCs usa um multicast domain do Transit Gateway. SiteLink liga escritórios entre si pela rede da AWS via Direct Connect, sem passar por uma região.

Macetes para memorizar

Associação x propagação

Associação: qual tabela eu leio. Propagação: em qual tabela eu apareço.

Escolha de conectividade

Poucas e pesadas: peering. Muitas e transitivas: TGW. Global por política: Cloud WAN. Só um serviço: PrivateLink.

Borda

Cache e HTTP: CloudFront. IP fixo, UDP e failover: Global Accelerator.

Peering de TGW

Entre TGWs não tem BGP nem propagação: rota estática dos dois lados.

Direct Connect resiliente

Dois lugares, dois dispositivos, dois roteadores, BGP.

Endpoints

Gateway endpoint: só S3 e DynamoDB, só de dentro da VPC. O resto é interface.

CIDR sobreposto

Quer conversar: NAT privado. Quer servir: PrivateLink. Quer microsserviços com IAM: Lattice.

Tabela de memorização: não confunda

Quando é...	...e quando é
Transit Gateway Muitas VPCs, várias contas, roteamento transitivo, integração com VPN e Direct Connect, controle central de rotas.	**VPC peering** Poucas VPCs sem sobreposição e muito tráfego: menor custo, sem processamento por GB e menor latência.
Transit Gateway com peering Hub regional com tabelas próprias, já existente, com peering e rotas estáticas entre regiões.	**AWS Cloud WAN** WAN global com segmentação declarativa por política central, sem configurar região a região.
AWS Global Accelerator IPs estáticos, TCP ou UDP (inclusive jogos), failover rápido entre regiões.	**Amazon CloudFront** Conteúdo HTTP/HTTPS com cache na borda, TLS e WAF centralizado.
AWS PrivateLink Expor um serviço atrás de NLB a muitas VPCs ou clientes, com acesso iniciado só pelo consumidor.	**Amazon VPC Lattice** Malha de serviços de aplicação entre VPCs e contas com auth policies do IAM e CIDRs sobrepostos.
NAT gateway privado CIDRs sobrepostos e aplicações de uma VPC iniciando conexões para outra rede.	**PrivateLink** CIDRs sobrepostos e o objetivo é só expor um serviço.

Local Zone Latência de poucos milissegundos para usuários de uma metrópole específica.	**Wavelength** Latência baixa para usuários móveis 5G.
Gateway endpoint do S3 Tráfego originado dentro da VPC, sem custo.	**Interface endpoint do S3** Acesso privado ao S3 a partir do on-premises ou de outra rede.

Números que caem

Item	Valor
Prefixo do NAT64 roteado para o NAT gateway	**64:ff9b::/96**
Faixa não roteável usada como CIDR secundário para pods do EKS	**100.64.0.0/10 (por exemplo, 100.64.0.0/16)**
Conexões de VPC peering em malha completa	**N*(N-1)/2**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Ativar a propagação das VPCs no Transit Gateway para o data center aprender as rotas pelo transit VIF.
Como não cair: O que o on-premises aprende é a lista de allowed prefixes da associação DXGW-TGW.

⚠ **Alerta de prova:** Contar com o DNS privado do endpoint para as VPCs spoke resolverem o endpoint centralizado.
Como não cair: O DNS privado só vale na VPC do endpoint. Desative-o e associe private hosted zones às spokes.

⚠ **Alerta de prova:** Usar VPC peering com uma VPC central para compartilhar NAT gateway ou internet.
Como não cair: Peering não é transitivo. Egress centralizado é via Transit Gateway.

⚠ **Alerta de prova:** Montar Transit Gateway para duas VPCs com dezenas de terabytes por mês.
Como não cair: O Transit Gateway cobra por GB processado. Para poucas VPCs e muito tráfego, VPC peering.

⚠ **Alerta de prova:** Criar peering ou Transit Gateway entre VPCs com CIDRs sobrepostos.
Como não cair: Ambos exigem CIDRs distintos. Use NAT gateway privado, PrivateLink ou VPC Lattice conforme o requisito.

⚠ **Alerta de prova:** Usar LAG em uma única localização Direct Connect para resiliência máxima.
Como não cair: Resiliência máxima exige pelo menos duas localizações, com conexões em dispositivos separados.

⚠ **Alerta de prova:** Usar Route 53 com roteamento por latência para obter IPs estáticos e failover rápido.
Como não cair: DNS não dá IPs estáticos e o failover depende do cache. A resposta é Global Accelerator.

⚠ **Alerta de prova:** Colocar CloudFront na frente de tráfego UDP de jogos.
Como não cair: CloudFront atende HTTP e HTTPS. UDP global: Global Accelerator.

⚠ **Alerta de prova:** Restringir o security group do ALB público à prefix list do CloudFront quando o requisito é ALB sem endereço público.
Como não cair: O ALB continuaria público. Use ALB interno como VPC origin.

⚠ **Alerta de prova:** Rotear ::/0 para um egress-only internet gateway para alcançar APIs só IPv4.
Como não cair: Egress-only é só IPv6. Use DNS64 e rota 64:ff9b::/96 para NAT gateway público.

⚠ **Alerta de prova:** Achar que configurar QoS em rotas ou BGP prioriza tráfego no Direct Connect.
Como não cair: QoS no Direct Connect só existe nos seus roteadores; a AWS preserva DSCP, mas não prioriza.

⚠ **Alerta de prova:** Associar o Network Firewall ao listener do ALB para inspecionar entrada da internet.
Como não cair: Inspeção de entrada exige ingress routing: tabela associada ao internet gateway (edge association) apontando para os endpoints do firewall, com retorno simétrico.

⚠ **Alerta de prova:** Usar prefix lists compartilhadas para evitar sobreposição de CIDRs.
Como não cair: Prefix lists não alocam blocos. Planejamento central de CIDRs é VPC IPAM.

⚠ **Alerta de prova:** Usar um NLB UDP para distribuir multicast a centenas de instâncias.
Como não cair: O NLB entrega cada pacote a um só alvo. Multicast é Transit Gateway multicast domain.

Como cai na prova

📝 **Como cai:** Empresa com muitas VPCs em várias contas e regiões, com malha de peering difícil de manter, pede o desenho mais escalável.
Como resolver: Um Transit Gateway por região, compartilhado pelo RAM, peering entre regiões e tabelas de rotas por ambiente. Se o enunciado falar em política global declarativa e segmentos, troque por Cloud WAN. Elimine malha de peering, VPN entre VPCs e roteador em EC2.

📝 **Como cai:** Conectividade híbrida com requisitos de banda, latência previsível e alta disponibilidade.
Como resolver: Direct Connect como caminho principal, em localizações distintas para resiliência, chegando a um Direct Connect gateway associado ao Transit Gateway, com BGP; VPN como backup quando pedido. Descarte VPN pela internet como principal e conexão hospedada de banda insuficiente.

📝 **Como cai:** Usuários globais, baixa latência e alta disponibilidade entre regiões.
Como resolver: Pergunte o protocolo e o requisito: HTTP com cache e WAF central vai de CloudFront; IPs estáticos, UDP ou failover rápido vai de Global Accelerator com NLBs ou ALBs regionais.

📝 **Como cai:** Duas redes com o mesmo CIDR precisam se comunicar e renumerar não é possível.
Como resolver: Identifique quem inicia e o escopo: fluxo iniciado por um lado usa CIDR secundário roteável com NAT gateway privado; um serviço exposto a muitos clientes usa PrivateLink; serviços de aplicação com IAM usam VPC Lattice.

📝 **Como cai:** Cenário simples com poucas VPCs na mesma região e conta.
Como resolver: Não superdimensione: VPC peering costuma ser a resposta. Transit Gateway só vence quando há muitas VPCs, várias contas ou necessidade de trânsito.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
dezenas de VPCs, várias contas, roteamento centralizado, adicionar VPCs sem novos peerings	**Transit Gateway compartilhado pelo RAM**
segmentos globais definidos em política central, sem peering região a região	**AWS Cloud WAN**
duas VPCs, sem planos de crescer, menor custo, muito tráfego	**VPC peering**
on-premises não recebe rotas das VPCs novas atrás do Transit Gateway	**Allowed prefixes da associação DXGW-TGW**
sobreviver à perda de uma localização Direct Connect inteira	**Conexões dedicadas em pelo menos duas localizações distintas**
IPs estáticos para liberar em firewalls, failover entre regiões, UDP	**AWS Global Accelerator**

ALB sem IP público entregue globalmente	**CloudFront com VPC origins**
CIDRs sobrepostos, acesso privado iniciado só pelos clientes a uma API	**PrivateLink com NLB**
comunicação entre serviços com IAM, CIDRs sobrepostos, sem gerenciar rotas	**Amazon VPC Lattice**
alocar CIDRs de forma central sem sobreposição	**Amazon VPC IPAM**
sub-redes IPv6-only acessando APIs só IPv4	**DNS64 + 64:ff9b::/96 para NAT gateway público**
mesma configuração de DNS (zonas, regras, DNS Firewall) em muitas VPCs e contas	**Route 53 Profiles compartilhados pelo RAM**
SD-WAN no Transit Gateway sem IPsec, roteamento dinâmico	**Transit Gateway Connect attachment (GRE + BGP)**
escritório a escritório pela rede da AWS via Direct Connect	**SiteLink**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Transit Gateway é regional: entre regiões, peering de TGW com rotas estáticas, ou Cloud WAN.
- VPC peering não é transitivo e não aceita CIDRs sobrepostos.
- On-premises aprende rotas do Transit Gateway pelos allowed prefixes da associação com o Direct Connect gateway.
- Resiliência máxima do Direct Connect exige pelo menos duas localizações.

Essenciais para a prova (checklist)

- ☐ Sei explicar associação e propagação nas tabelas do Transit Gateway.
- ☐ Sei quando escolher Transit Gateway, Cloud WAN, VPC peering, PrivateLink e VPC Lattice.
- ☐ Sei desenhar Direct Connect com Direct Connect gateway, Transit Gateway e o tipo de VIF correto.
- ☐ Sei o que define as rotas anunciadas ao on-premises numa associação DXGW-TGW.
- ☐ Sei montar egress centralizado e por que peering não serve para isso.
- ☐ Sei resolver CIDRs sobrepostos conforme quem inicia a conexão.
- ☐ Sei centralizar interface endpoints mantendo a resolução dos nomes padrão.
- ☐ Sei escolher entre CloudFront e Global Accelerator.
- ☐ Sei configurar acesso de sub-redes IPv6-only a destinos IPv4.

Questões de revisão do capítulo

R1.1 · Network Design

Uma empresa de jogos online precisa fornecer baixa latência e alta disponibilidade para jogadores distribuídos globalmente. Os servidores de aplicação rodam em múltiplas VPCs em diferentes regiões AWS, atrás de Application Load Balancers (ALBs). A empresa também precisa proteger a infraestrutura contra ataques DDoS e aplicar regras de segurança em nível de aplicação (camada 7) com um único ponto de gerenciamento. Qual é o design de rede MAIS adequado para atender esses requisitos?

A. Criar VPNs site-to-site de cada região AWS para um data center central, concentrar todo o tráfego dos jogadores nesse data center e então encaminhar para as VPCs por túneis GRE, aplicando firewall tradicional de camada 7 on-premises.
B. Colocar o CloudFront na frente dos ALBs das regiões, com uma Web ACL do AWS WAF associada a ele e o AWS Shield para mitigar ataques DDoS
C. Usar AWS Global Accelerator para distribuir o tráfego para os ALBs em cada região, associando um AWS WAF em cada ALB individualmente.
D. Configurar um Amazon Route 53 com política de roteamento geolocalizado apontando diretamente para os ALBs em cada região, sem uso de serviços adicionais, e aplicar regras de segurança somente em Security Groups.

R1.2 · Network Design

Uma empresa quer que o time de rede controle CIDRs, rotas, NAT e conectividade, enquanto dezenas de times de aplicação, cada um em sua conta, só criam recursos em sub-redes padronizadas. Ela também quer reduzir o número de VPCs e de attachments no Transit Gateway. Qual desenho atende?

A. Criar VPCs em cada conta por StackSets e bloquear alterações de rede com SCPs nas contas
B. Criar VPCs na conta de rede e compartilhar as sub-redes com as contas dos times pelo AWS RAM
C. Criar uma VPC por conta de aplicação e anexá-las a um Transit Gateway compartilhado entre contas
D. Criar uma única conta para todos os times, separando as permissões com políticas do IAM por tags

R1.3 · Network Design

Uma empresa está projetando uma arquitetura em múltiplas regiões AWS para um aplicativo crítico que exige alta disponibilidade e baixa latência global. A empresa já utiliza AWS Transit Gateway em cada região para conectar várias VPCs locais. O time de arquitetura deseja interconectar as regiões de forma escalável, com gerenciamento centralizado de rotas, evitando a complexidade de múltiplos emparelhamentos de VPC entre regiões. Qual é a abordagem de design MAIS adequada para atender a esses requisitos?

A. Usar AWS Direct Connect com múltiplos links físicos entre as regiões e configurar rotas BGP diretamente entre as VPCs.
B. Configurar AWS Site-to-Site VPN entre as VPCs de cada região e usar rotas estáticas para interconectar as redes.
C. Criar emparelhamento de VPC (VPC peering) entre as VPCs das diferentes regiões e configurar rotas à mão em cada tabela de rotas.
D. Interligar os Transit Gateways das regiões por peering e adicionar rotas estáticas para as VPCs remotas

R1.4 · Network Design

Uma empresa tem 60 VPCs e cria interface endpoints dos mesmos serviços (como SQS, KMS e STS) em cada uma, o que custa caro. As VPCs estão anexadas a um Transit Gateway. Como centralizar esses endpoints mantendo a resolução dos nomes padrão dos serviços?

A. Criar os endpoints em uma VPC compartilhada sem DNS privado e associar às VPCs spoke private hosted zones com os nomes dos serviços
B. Criar os endpoints na VPC compartilhada com DNS privado ativado e deixar as spokes resolverem os nomes pelo Transit Gateway
C. Remover os endpoints e acessar os serviços pela internet por NAT gateways centralizados na VPC de egress
D. Usar gateway endpoints para SQS, KMS e STS em cada VPC, já que eles não têm custo por hora

Respostas comentadas

R1.1. B) Colocar o CloudFront na frente dos ALBs das regiões, com uma Web ACL do AWS WAF associada a ele e o AWS Shield para mitigar ataques DDoS

Por quê: Esta alternativa é a mais adequada porque combina baixa latência global, alta disponibilidade e segurança centralizada. O Amazon CloudFront utiliza a rede global edge da AWS para aproximar o tráfego do usuário, reduzindo a latência percebida. Ao colocar o CloudFront na frente dos ALBs em múltiplas regiões, é possível distribuir o tráfego de forma eficiente e tirar proveito de caching quando aplicável.

✗ A) Incorreta. Centralizar o tráfego em um data center on-premises adiciona latência desnecessária para usuários globais, cria um potencial ponto único de falha e complica o design de rede com múltiplos túneis (VPN + GRE).

✗ C) Incorreta. O AWS Global Accelerator melhora latência e disponibilidade usando a rede global da AWS, mas associar WAF individualmente em cada ALB fragmenta o gerenciamento de segurança.

✗ D) Incorreta. Depender apenas de Route 53 com roteamento geolocalizado não fornece aceleração de borda nem mecanismos avançados de mitigação DDoS em nível de aplicação.

> **Dica de prova:** Quando o enunciado mencionar simultaneamente: (1) usuários globais, (2) baixa latência, (3) alta disponibilidade entre múltiplas regiões e (4) proteção DDoS com regras de camada 7 centralizadas, pense em combinar Amazon CloudFront + AWS WAF + AWS Shield como a solução padrão na borda.

R1.2. B) Criar VPCs na conta de rede e compartilhar as sub-redes com as contas dos times pelo AWS RAM

Por quê: No VPC sharing, a conta dona da VPC compartilha sub-redes pelo AWS RAM com contas da mesma organização. Os participantes criam instâncias, bancos e load balancers nessas sub-redes, mas não alteram a VPC, as rotas ou os gateways. Isso centraliza a rede e reduz VPCs e attachments.

✗ A) Incorreta. Padroniza, mas não reduz o número de VPCs nem de attachments.

✗ C) Incorreta. Mantém uma VPC e um attachment por conta, que é o que se quer reduzir.

✗ D) Incorreta. Perde o isolamento de contas, que continua desejável.

> **Dica de prova:** Time de rede no controle e contas de aplicação só usando sub-redes: VPC sharing pelo RAM.

R1.3. D) Interligar os Transit Gateways das regiões por peering e adicionar rotas estáticas para as VPCs remotas

Por quê: Esta alternativa é a mais adequada porque o peering entre AWS Transit Gateways permite interconectar, de forma escalável, várias VPCs em múltiplas regiões. Cada VPC continua anexada ao seu Transit Gateway local, e as rotas podem ser propagadas para as tabelas de rotas do Transit Gateway, simplificando o gerenciamento. Isso evita a malha complexa de VPC peering entre contas e regiões e mantém um backbone privado da AWS com baixa latência e alta disponibilidade.

✗ A) Incorreta. AWS Direct Connect é voltado para conectar o data center on-premises à AWS. Não é projetado para interconectar diretamente VPCs entre regiões;

✗ B) Incorreta. Site-to-Site VPN entre VPCs adiciona overhead de criptografia, maior latência e limitações de throughput em comparação com o backbone privado da AWS.

✗ C) Incorreta. VPC peering entre todas as VPCs em múltiplas regiões não escala bem. Exige configuração de uma malha completa de emparelhamentos e atualizações manuais de rotas em múltiplas tabelas, aumentando complexidade operacional e risco...

> **Dica de prova:** Quando já existe AWS Transit Gateway em cada região e o objetivo é interligar várias VPCs entre regiões com simplicidade e escala, pense em peering entre Transit Gateways. Use VPC peering apenas para poucas conexões diretas e simples; para topologias maiores, Transit Gateway tende a ser mais adequado.

R1.4. A) Criar os endpoints em uma VPC compartilhada sem DNS privado e associar às VPCs spoke private hosted zones com os nomes dos serviços

Por quê: Para centralizar interface endpoints, eles ficam em uma VPC de serviços compartilhados com o DNS privado desativado, e private hosted zones com os nomes dos serviços (alias para o endpoint) são associadas às VPCs spoke, que chegam ao endpoint pelo Transit Gateway.

✗ B) Incorreta. O DNS privado do endpoint só vale na VPC onde ele foi criado; as spokes continuariam resolvendo para os IPs públicos.

✗ C) Incorreta. Leva o tráfego à internet, com custo de NAT e fora do requisito de privacidade.

✗ D) Incorreta. Gateway endpoints existem só para S3 e DynamoDB.

> **Dica de prova:** Endpoints centralizados: private hosted zones associadas às VPCs spoke; o DNS privado do endpoint não se propaga para outras VPCs.

02

CAPÍTULO 2 · 26% DA PROVA

Network Implementation

Implementação é onde a prova testa se eu sei configurar de verdade: atributos BGP para engenharia de tráfego, VPN com ECMP, opções de túnel, MTU, DNS híbrido com Route 53 Resolver, appliance mode, rotas no peering de Transit Gateway e detalhes de balanceadores. Os enunciados costumam descrever um sintoma (o tráfego sai pela VPN, o túnel cai sem tráfego, as regiões não se alcançam) e pedir a configuração exata que falta. A outra metade é automação: CloudFormation StackSets, pipelines com aprovação e Systems Manager. Onde mais erro: inverter a direção do controle BGP (local preference controla a saída do meu data center; communities e AS path controlam o que vem da AWS).

Neste capítulo
18 tópicos-chave · 13 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Local preference no roteador on-premises

Controla o tráfego que sai do data center para a AWS. Para preferir o Direct Connect à VPN, atribua local preference maior às rotas recebidas pelo BGP do Direct Connect. Rotas do Transit Gateway controlam o tráfego que sai da AWS, não o que sai do data center.

BGP communities 7224:7x00

Controlam o tráfego da AWS para o on-premises entre conexões Direct Connect sem mudar os prefixos: 7224:7300 marca a preferência alta e 7224:7100 a baixa. Alternativas para atrair tráfego da AWS são prefixos mais específicos; AS path prepending torna a rota menos atrativa.

Direct Connect com VPN de backup

Com DX e VPN no mesmo gateway anunciando o mesmo prefixo, a AWS prefere o Direct Connect. O Direct Connect sempre usa BGP; a VPN com BGP permite failover automático, e AS path maior na VPN reforça a preferência pelo DX.

ECMP em VPN com Transit Gateway

Para somar a banda de vários túneis, crie várias VPNs com BGP para o Transit Gateway e ative ECMP nele e no roteador on-premises. O virtual private gateway não suporta ECMP entre túneis. Cada túnel padrão tem limite de banda de cerca de 1,25 Gbps; mais banda vem de somar túneis.

VPN acelerada

Disponível com Transit Gateway, faz o túnel entrar na rede da AWS pela borda mais próxima, melhorando desempenho em longas distâncias. Não remove o limite de banda de cada túnel.

Opções de túnel da VPN

Para um túnel que cai quando fica sem tráfego, configure startup action como Start (a AWS inicia a negociação) e DPD timeout action como Restart. Com roteador on-premises sem suporte a BGP, use VPN com roteamento estático no VGW ou no Transit Gateway.

MTU na AWS

9001 bytes dentro da VPC e no peering da mesma região, 8500 no Transit Gateway entre VPCs e 1500 na VPN Site-to-Site e na internet. O MTU deve respeitar o menor valor do caminho; túneis VPN não aceitam 9001.

Route 53 Resolver endpoints

Inbound endpoint permite que o on-premises consulte nomes da AWS; outbound endpoint com forwarding rule permite que a VPC resolva domínios on-premises como corp.local. O resolver .2 da VPC não aceita consultas vindas de fora dela. Em multi-conta, endpoints em conta central e regras compartilhadas pelo RAM.

Private hosted zone entre contas

Crie na conta dona da zona uma autorização para cada VPC e, na conta da VPC, associe a VPC à zona. Zona pública para domínio interno expõe nomes e não resolve o encaminhamento.

Appliance mode

Ativado no attachment da VPC de inspeção do Transit Gateway, mantém os dois sentidos de um fluxo no mesmo appliance, evitando descarte de estado em firewalls stateful com tráfego assimétrico. O Transit Gateway roteia, não filtra portas.

Rotas no peering de Transit Gateway

Peering attachments não suportam propagação e não há BGP entre os Transit Gateways. Se as regiões não se alcançam mesmo com propagação ativa, faltam rotas estáticas para os CIDRs remotos apontando para o peering attachment nos dois lados.

Referência de security group entre VPCs

Para aceitar conexões referenciando o security group de outra VPC em vez de CIDRs, use VPC peering ou ative o suporte a security group referencing no Transit Gateway e nos attachments, na mesma região.

IP de origem no NLB

Com preservação de IP do cliente desativada, o alvo vê IPs privados do NLB. Sem mudar o tipo de alvo, ative Proxy Protocol v2 no target group e prepare a aplicação para ler o cabeçalho. X-Forwarded-For é cabeçalho HTTP do ALB.

ALB com alvos em outras VPCs

Um ALB internet-facing numa VPC central pode usar target groups do tipo IP com os IPs privados das instâncias de VPCs de backend alcançadas pelo Transit Gateway. ALB não aceita Elastic IP; IP estático vem do NLB ou do Global Accelerator.

Políticas de VPC endpoint para S3

Para evitar exfiltração pela VPC, a política do gateway endpoint permite só buckets da organização com aws:ResourceOrgID. Para proteger o bucket, a bucket policy exige aws:SourceVpce. O gateway endpoint é associado às tabelas de rotas das sub-redes.

Saída para a internet: NAT gateway e egress-only

IPv4: NAT gateway em sub-rede pública com Elastic IP, rota 0.0.0.0/0 da sub-rede pública para o internet gateway anexado à VPC e rota padrão das privadas para o NAT. IPv6 sem entrada: egress-only internet gateway com rota ::/0; IPv6 não usa NAT para saída.

Rede de containers

No ECS, o modo awsvpc dá uma ENI e IP próprio a cada task, com security group por task e visibilidade nos flow logs; bridge e host compartilham o IP do host. No EKS, o Amazon VPC CNI dá aos pods IPs da VPC; para esgotamento de IPs, CIDR secundário não roteável com custom networking.

Automação de rede

CloudFormation StackSets com implantação automática na organização padroniza VPCs, attachments, flow logs e alarmes em contas e regiões. Mudanças seguem pipeline (CodePipeline com validação no CodeBuild e aprovação manual para produção). Configurações de appliances podem ser versionadas com Systems Manager State Manager e Parameter Store ou AppConfig.

Macetes para memorizar

💡 Direção do BGP

Local preference olha para fora (saída do meu DC); communities e AS path olham para dentro (o que a AWS me manda).

💡 Communities

7300 é o topo, 7100 é o fundo: quanto maior o número, mais preferida a conexão.

💡 MTU

9001 na VPC, 8500 no TGW, 1500 na VPN e na internet: descendo a escada conforme sai da VPC.

💡 Resolver

Inbound: o de fora pergunta para a AWS. Outbound: a AWS pergunta para o de fora.

ECMP

ECMP mora no Transit Gateway; o VGW não sabe somar túneis.

Túnel que dorme

Start para acordar, Restart quando o DPD estourar.

IP do cliente

ALB conta no cabeçalho (X-Forwarded-For); NLB conta no protocolo (Proxy Protocol v2).

Tabela de memorização: não confunda

Quando é...	...e quando é
Local preference Controlar o tráfego que sai do data center para a AWS.	**Communities 7224:7x00, AS path ou prefixo mais específico** Controlar o tráfego que vem da AWS para o data center.
VPN no Transit Gateway Somar banda de túneis com ECMP, VPN acelerada e várias VPCs.	**VPN no virtual private gateway** Cenário simples de uma VPC, sem ECMP.
Route 53 Resolver inbound endpoint O on-premises precisa resolver nomes da AWS.	**Route 53 Resolver outbound endpoint** As VPCs precisam resolver domínios on-premises por forwarding rules.
Proxy Protocol v2 NLB com listener TCP repassando o IP de origem do cliente.	**X-Forwarded-For** ALB inserindo o IP do cliente no cabeçalho HTTP.
Política do gateway endpoint (aws:ResourceOrgID) Impedir que instâncias da VPC enviem dados a buckets fora da organização.	**Bucket policy (aws:SourceVpce)** Garantir que o bucket só seja acessado pelo VPC endpoint.
Egress-only internet gateway Saída IPv6 sem permitir conexões iniciadas da internet.	**NAT gateway** Saída IPv4 de sub-redes privadas, ou NAT64 para destinos IPv4.

Números que caem

Item	Valor
MTU dentro da VPC e no peering da mesma região	**9001 bytes**
MTU no Transit Gateway entre VPCs	**8500 bytes**
MTU na VPN Site-to-Site e na internet	**1500 bytes**
Community BGP de preferência alta no Direct Connect	**7224:7300**

Community BGP de preferência baixa no Direct Connect	**7224:7100**
Limite de banda de cada túnel padrão de VPN Site-to-Site	**cerca de 1,25 Gbps**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Criar rotas estáticas no Transit Gateway para fazer o data center preferir o Direct Connect.
Como não cair: Rotas do TGW controlam a saída da AWS. A saída do data center se controla com local preference no roteador on-premises.

⚠ **Alerta de prova:** Aplicar AS path prepending nas rotas da conexão que deve ser a principal.
Como não cair: Prepending deixa a rota menos atrativa. Para a principal, community 7224:7300; para a backup, 7224:7100.

⚠ **Alerta de prova:** Anunciar prefixos mais específicos pela conexão de backup.
Como não cair: Prefixo mais específico atrai o tráfego para essa conexão, o oposto do desejado.

⚠ **Alerta de prova:** Ativar ECMP no virtual private gateway com várias VPNs estáticas.
Como não cair: VGW não faz ECMP. Use várias VPNs com BGP no Transit Gateway.

⚠ **Alerta de prova:** Achar que VPN acelerada remove o limite de banda do túnel.
Como não cair: Ela só melhora o caminho pela internet; mais banda vem de ECMP com várias VPNs.

⚠ **Alerta de prova:** Aumentar o MTU dos túneis VPN para 9001.
Como não cair: VPN e internet aceitam no máximo 1500; o Transit Gateway, 8500.

⚠ **Alerta de prova:** Ativar propagação no peering attachment ou criar sessão BGP entre Transit Gateways.
Como não cair: Peering de TGW não suporta nenhum dos dois: use rotas estáticas nos dois lados.

⚠ **Alerta de prova:** Fazer o on-premises consultar o resolver .2 da VPC pela VPN.
Como não cair: O .2 não aceita consultas de fora da VPC. Use inbound endpoint do Resolver.

⚠ **Alerta de prova:** Habilitar X-Forwarded-For no listener TCP do NLB.
Como não cair: O NLB não insere esse cabeçalho. Use Proxy Protocol v2 ou preservação do IP do cliente.

⚠ **Alerta de prova:** Usar appliance mode para referenciar security groups entre VPCs.
Como não cair: Appliance mode trata simetria de fluxos. Referência de SG exige o suporte específico ativado no Transit Gateway.

⚠ **Alerta de prova:** Criar NAT gateway com rota ::/0 para saída IPv6.
Como não cair: IPv6 não usa NAT para saída; use egress-only internet gateway.

⚠ **Alerta de prova:** Associar Elastic IP a um ALB para ter IP fixo.
Como não cair: ALB não suporta Elastic IP. Use NLB ou Global Accelerator para IPs estáticos.

⚠ **Alerta de prova:** Filtrar portas 80 e 443 entre VPCs no próprio Transit Gateway.
Como não cair: O Transit Gateway roteia, não filtra. Filtro central exige VPC de inspeção com firewall e appliance mode.

Como cai na prova

📝 **Como cai:** Sintoma de roteamento híbrido: o tráfego usa o caminho errado entre Direct Connect e VPN.
Como resolver: Descubra a direção. Saindo do data center: local preference no roteador on-premises. Vindo da AWS: communities 7224:7x00, prefixo mais específico ou AS path maior no caminho de backup. Rejeite rotas estáticas que eliminam failover.

📝 **Como cai:** Algo foi configurado e não funciona; qual é o passo que falta?
Como resolver: Liste o que o recurso não suporta: peering de TGW sem propagação nem BGP, VGW sem ECMP, DNS privado do endpoint preso à VPC, .2 sem consultas externas. A resposta é o passo manual que compensa a limitação.

📝 **Como cai:** DNS híbrido entre VPCs de várias contas e data center.
Como resolver: Endpoints inbound e outbound do Route 53 Resolver em conta central, regras de encaminhamento compartilhadas pelo RAM e associadas às VPCs. Descarte BIND em EC2 e zonas replicadas em cada conta.

📝 **Como cai:** Padronizar a implantação de rede em muitas contas e regiões com o menor erro manual.
Como resolver: CloudFormation StackSets com implantação automática na organização, versionado em pipeline com validação e aprovação manual para produção. Rejeite console com runbook, scripts bash com credenciais e AMIs por mudança.

📝 **Como cai:** Expor uma aplicação com detalhes de balanceador, IP de origem ou IP estático.
Como resolver: HTTP/HTTPS com instâncias privadas: ALB em sub-redes públicas de ao menos duas AZs. IP real no NLB: Proxy Protocol v2. IP estático: NLB ou Global Accelerator, nunca Elastic IP no ALB.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
o tráfego do data center às vezes sai pela VPN em vez do Direct Connect	**Local preference maior para rotas do DX no roteador on-premises**
tráfego da AWS deve usar a conexão A e deixar a B como backup sem mudar prefixos	**Communities 7224:7300 na A e 7224:7100 na B**
somar banda de vários túneis VPN enquanto o Direct Connect não fica pronto	**Várias VPNs com BGP e ECMP no Transit Gateway**
VPN com desempenho ruim em longas distâncias	**VPN acelerada com Transit Gateway**
túnel VPN cai quando fica sem tráfego	**Startup action Start e DPD timeout action Restart**
Transit Gateways em regiões com peering, propagação ativa, VPCs não se alcançam	**Rotas estáticas para o peering attachment nos dois lados**
instâncias precisam resolver corp.local hospedado on-premises	**Outbound endpoint do Resolver com forwarding rule**
firewall stateful atrás do Transit Gateway descarta tráfego assimétrico	**Appliance mode no attachment da VPC de inspeção**
NLB, aplicação precisa do IP real do cliente sem mudar o tipo de alvo	**Proxy Protocol v2 no target group**
pacotes grandes perdidos entre VPCs pelo TGW ou na VPN	**MTU 8500 no Transit Gateway e 1500 na VPN**
mesmo /24 próprio anunciado globalmente com failover entre regiões	**BYOIP no Global Accelerator**
tasks do ECS com IP próprio e security group por task	**Modo de rede awsvpc**
evitar exfiltração para buckets de fora da organização	**Política do gateway endpoint com aws:ResourceOrgID**
detecção rápida de falha nas sessões BGP do Direct Connect	**BFD em cada sessão BGP**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Local preference controla a saída do data center; communities, AS path e prefixos mais específicos controlam o que vem da AWS.
- Peering de Transit Gateway: rotas estáticas dos dois lados, sem propagação e sem BGP.
- ECMP de VPN só no Transit Gateway, com BGP.

Essenciais para a prova (checklist)

- ☐ Sei usar local preference, communities 7224:7x00, AS path e prefixos mais específicos na direção correta.
- ☐ Sei por que a AWS prefere o Direct Connect à VPN para o mesmo prefixo.
- ☐ Sei configurar ECMP em VPN e sei que o VGW não suporta.
- ☐ Sei as opções de túnel que mantêm a VPN de pé sem tráfego.
- ☐ Sei os valores de MTU dentro da VPC, no Transit Gateway e na VPN.
- ☐ Sei configurar DNS híbrido com endpoints inbound e outbound e regras compartilhadas.
- ☐ Sei associar uma private hosted zone a VPCs de outra conta.
- ☐ Sei completar o roteamento de um peering entre Transit Gateways.
- ☐ Sei obter o IP real do cliente atrás de um NLB.
- ☐ Sei padronizar a rede em várias contas com StackSets e pipeline.

Questões de revisão do capítulo

R2.1 · Network Implementation

Uma empresa recebe as mesmas rotas da AWS por Direct Connect e por uma VPN Site-to-Site de backup, ambas terminando no mesmo Transit Gateway. O tráfego do data center para a AWS às vezes sai pela VPN. O time quer que ele use o Direct Connect e só vá para a VPN se o link falhar. O que deve ser feito?

A. Atribuir, no roteador on-premises, local preference maior às rotas recebidas pelo BGP do Direct Connect que às da VPN
B. Criar rotas estáticas no Transit Gateway apontando para a VPN, com prioridade menor que as rotas propagadas
C. Desativar o BGP na VPN e usar rotas estáticas, que o roteador on-premises trata como menos preferidas
D. Anunciar da AWS as rotas da VPN com AS path mais curto para que o roteador on-premises passe a preferi-las

R2.2 · Network Implementation

Uma fintech precisa expor uma aplicação rodando em uma VPC privada na região sa-east-1 para clientes corporativos conectados via AWS Direct Connect a partir de múltiplas contas e regiões. Os requisitos são: - Acessar a aplicação usando nomes DNS amigáveis, com resolução interna para os clientes on-premises. - Evitar roteamento assimétrico e dependência de roteamento transitive entre VPCs. - Permitir que novas contas AWS consumam o serviço sem alterar a VPC da aplicação. Qual arquitetura atende melhor a esses requisitos?

A. Configurar peering VPC full-mesh entre a VPC da aplicação e as VPCs das contas consumidoras, utilizar um NLB interno e criar uma Private Hosted Zone do Route 53 associada a as VPCs, propagando as rotas entre on-premises e as VPCs por meio de BGP no Direct Connect Gateway.
B. Criar um Transit Gateway centralizado, anexar a VPC da aplicação e as VPCs das contas consumidoras, usar um ALB interno na VPC da aplicação.
C. Usar um NLB interno publicado pelo PrivateLink às contas consumidoras, com uma private hosted zone para o nome do serviço e endpoints do Resolver para o on-premises
D. Criar um Application Load Balancer (ALB) na VPC da aplicação, publicar um endpoint público e usar Route 53 Public Hosted Zone com registros A, configurando regras de firewall on-premises para restringir o acesso só pelos IPs das filiais.

R2.3 · Network Implementation

VPCs da mesma região estão ligadas por um Transit Gateway. O time quer que o security group dos bancos na VPC de dados aceite conexões referenciando o security group das aplicações de outra VPC, em vez de listar CIDRs. O que habilitar?

A. O suporte a security group referencing no Transit Gateway e nos attachments das VPCs envolvidas
B. O DNS support no Transit Gateway, para que os nomes dos security groups sejam resolvidos
C. O appliance mode nos attachments das VPCs, para manter as conexões simétricas entre as zonas de disponibilidade
D. Um VPC peering entre as VPCs, já que referências entre VPCs só funcionam por peering

R2.4 · Network Implementation

Um engenheiro de redes precisa conectar uma VPC de produção na região us-east-1 a uma VPC de testes na mesma conta e região, garantindo baixa latência e alta largura de banda, sem necessidade de criptografia adicional. Qual solução é MAIS adequada para essa necessidade?

A. Criar um AWS Site-to-Site VPN entre as duas VPCs usando gateways de trânsito
B. Configurar um VPC peering diretamente entre as duas VPCs e atualizar as tabelas de rotas
C. Criar um AWS Direct Connect entre as duas VPCs utilizando um provedor parceiro
D. Criar endpoints de interface (AWS PrivateLink) em cada VPC para acesso bidirecional

Respostas comentadas

R2.1. A) Atribuir, no roteador on-premises, local preference maior às rotas recebidas pelo BGP do Direct Connect que às da VPN

Por quê: O tráfego do data center para a AWS segue a decisão do roteador on-premises. Local preference é o atributo BGP que define o caminho de saída: um valor maior para as rotas do Direct Connect mantém a VPN como backup.

✗ B) Incorreta. Rotas do Transit Gateway controlam o tráfego que sai da AWS, não o que sai do data center.

✗ C) Incorreta. Rotas estáticas não ficam menos preferidas por padrão no roteador on-premises e eliminam o failover dinâmico.

✗ D) Incorreta. Isso faria o data center preferir a VPN, o oposto do desejado.

> **Dica de prova:** Saída do on-premises: local preference. Entrada vinda da AWS: AS path, prefixos mais específicos ou communities.

R2.2. C) Usar um NLB interno publicado pelo PrivateLink às contas consumidoras, com uma private hosted zone para o nome do serviço e endpoints do Resolver para o on-premises

Por quê: Esta alternativa é a mais adequada porque combina AWS PrivateLink com DNS privado e integração com on-premises via Route 53 Resolver, atendendo a todos os requisitos: - O Network Load Balancer interno serve como ponto de entrada estável para a aplicação dentro da VPC da fintech. - PrivateLink (endpoint de serviço/interface) permite que múltiplas contas (e até múltiplas regiões, se suportado) consumam o serviço de forma privada, sem roteamento transitivo entre VPCs, evitando problemas de roteamento assimétrico.

✗ A) Incorreta. O peering full-mesh entre VPCs não escala bem em ambientes multi-account; além disso, utiliza roteamento transitivo indireto via Direct Connect e múltiplas VPCs, o que pode gerar roteamento assimétrico e complexidade...

✗ B) Incorreta. O Transit Gateway resolve parcialmente a conectividade L3 e a escalabilidade, mas não oferece o mesmo modelo de "serviço publicado" como PrivateLink.

✗ D) Incorreta. Expõe um endpoint público, o que viola a exigência de manter o acesso privado via Direct Connect e aumenta a superfície de ataque.

> **Dica de prova:** Quando o requisito é "publicar um serviço" (modelo provider/consumer) entre múltiplas contas ou até múltiplas regiões, com forte isolamento de rede e sem roteamento transitivo, pense em AWS PrivateLink + NLB interno.

R2.3. A) O suporte a security group referencing no Transit Gateway e nos attachments das VPCs envolvidas

Por quê: O Transit Gateway permite referenciar security groups entre VPCs da mesma região quando o recurso é ativado no Transit Gateway e nos VPC attachments. Não funciona por Transit Gateway peering entre regiões.

✗ B) Incorreta. DNS support resolve nomes DNS, não identificadores de security groups.

✗ C) Incorreta. Appliance mode trata simetria de fluxos para appliances, não referência de security groups.

✗ D) Incorreta. Peering também permite, mas o Transit Gateway já suporta o recurso, sem nova conexão.

> **Dica de prova:** Referenciar security groups entre VPCs: VPC peering ou Transit Gateway com o suporte ativado (mesma região).

R2.4. B) Configurar um VPC peering diretamente entre as duas VPCs e atualizar as tabelas de rotas

Por quê: Esta alternativa é a mais adequada porque o VPC peering oferece conectividade privada, de baixa latência e alta largura de banda entre duas VPCs na mesma região, sem custo adicional de criptografia e sem necessidade de infraestrutura física. Basta criar a conexão de peering e atualizar as tabelas de rotas em ambas as VPCs para permitir o tráfego.

✗ A) Incorreta. Criar um Site-to-Site VPN é desnecessário para VPCs na mesma região; isso adiciona complexidade, latência e custo com túneis IPsec, além de exigir virtual private gateways ou transit gateways.

✗ C) Incorreta. O Direct Connect é voltado para conectar ambientes on-premises à AWS, não é a solução típica para conectar VPCs na mesma região, sendo mais caro e complexo de operar.

✗ D) Incorreta. O AWS PrivateLink é ideal para expor serviços específicos (como endpoints de serviço), não para roteamento geral entre VPCs; não substitui o VPC peering para tráfego amplo e bidirecional de sub-redes.

Dica de prova: Use VPC peering para conectar VPCs na mesma região quando precisar de comunicação privada, de baixa latência e sem necessidade de recursos avançados de roteamento. Lembre-se de que VPC peering não é transitivo e exige atualização explícita das tabelas de rotas em ambas as VPCs.

03

CAPÍTULO 3 · 20% DA PROVA

Network Management and Operation

Neste domínio eu preciso saber qual ferramenta mede o quê: latência e perda, tráfego por fluxo, caminho lógico, topologia ou mudança de configuração. A prova adora oferecer CloudTrail, Config e Flow Logs como distratores para medir desempenho, o que nenhum deles faz. As respostas certas giram em torno da família CloudWatch (Network Monitor, Network Flow Monitor, Internet Monitor, Synthetics, métricas nativas e cross-account observability), do Network Manager com Route Analyzer e Infrastructure Performance e do Reachability Analyzer. Também cai muito centralização de logs em escala, com S3 + Athena para retenção longa. Meu erro mais comum é confundir as três ferramentas Monitor e escolher solução com agente quando o enunciado diz sem agentes.

Neste capítulo

18 tópicos-chave · 13 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

CloudWatch Network Monitor

Mede latência e perda de pacotes entre sub-redes de VPCs e destinos on-premises alcançados por Direct Connect ou VPN, com sondas e sem instalar agentes em nenhum dos lados. Métricas vão para dashboards e alarmes do CloudWatch. Não faz análise de trajeto entre serviços dentro da AWS.

CloudWatch Network Flow Monitor

Usa um agente nas instâncias para medir perda e tempo de ida e volta (RTT) por fluxo entre instâncias e VPCs, guardando o histórico e indicando em que trecho da rede está a degradação. É a resposta para desempenho entre workloads dentro da AWS.

CloudWatch Internet Monitor

Monitora desempenho e disponibilidade entre usuários na internet e aplicações expostas na AWS, com visão por local dos usuários e alarmes. Não monitora rotas BGP nem malhas internas entre VPCs.

Infrastructure Performance (Network Manager)

Mostra a latência agregada da própria rede da AWS entre regiões e entre AZs, sem instalar nada. Responde à pergunta: a rede da AWS ficou lenta naquele horário?

AWS Network Manager e global network

Registra Transit Gateways, VPNs, Direct Connect e dispositivos on-premises ou SD-WAN em uma global network, com visão de topologia. Envia eventos de mudança de rotas e de status ao EventBridge. O Route Analyzer verifica o caminho efetivo pelas tabelas do Transit Gateway, sem medir desempenho.

VPC Reachability Analyzer

Análise estática da configuração (rotas, security groups, NACLs, Transit Gateway) entre uma origem e um destino, mostrando o caminho salto a salto e o que bloqueia. Pode analisar entre contas pela integração com o Organizations. Não mede latência nem faz monitoramento contínuo.

VPC Flow Logs

Registram metadados de fluxo por VPC, sub-rede ou ENI: IPs, portas, protocolo, bytes, pacotes e ACCEPT/REJECT. Não medem latência nem perda e não geram métricas nativas no CloudWatch; é preciso metric filters para virar métrica e alarme. Podem ser entregues no CloudWatch Logs ou no S3 de uma conta central.

Transit Gateway Flow Logs

Dão visibilidade centralizada do tráfego que passa pelo Transit Gateway entre VPCs, VPNs e Direct Connect. Para retenção longa, envie ao S3 com particionamento (por hora, attachment, conta, região) e consulte com Athena. Não substituem os VPC Flow Logs para tráfego interno de uma VPC.

Métricas do Transit Gateway no CloudWatch

Métricas nativas por attachment como BytesIn, PacketDropCountNoRoute e PacketDropCountBlackhole, sem agentes. São a primeira escolha para volume, descarte por falta de rota e alarmes; o Transit Gateway não expõe SNMP nem permite tcpdump.

Métricas de VPN Site-to-Site

TunnelState, TunnelDataIn e TunnelDataOut no CloudWatch permitem alarmes de queda de túnel e dashboard central. Para mudanças de estado, EventBridge leva os eventos ao SNS ou ao Systems Manager Automation para mitigar.

Métricas nativas de rede do EC2

NetworkIn, NetworkOut, NetworkPacketsIn e NetworkPacketsOut são coletadas sem agente; detailed monitoring aumenta a granularidade. O CloudWatch guarda métricas por 15 meses, útil para tendência de capacidade. Limites do ENA exigem o CloudWatch Agent.

CloudWatch cross-account observability

Liga uma monitoring account central às source accounts pelo Observability Access Manager para ver métricas, logs e traces sem copiar dados nem escrever código. Alarmes e dashboards ficam na conta central. É a resposta padrão para observabilidade multi-conta e multi-região.

Traffic Mirroring

Copia os pacotes completos (payload) das ENIs para appliances de inspeção. Serve para depuração profunda, IDS e forense em fluxos selecionados; é caro e pesado para monitoramento contínuo ou de capacidade.

CloudWatch Synthetics

Canaries que chamam endpoints HTTP e APIs periodicamente, medindo disponibilidade e latência de aplicação, com alarmes. Podem rodar em VPC para testar endpoints privados e ALBs internos entre VPCs. Não medem perda de pacotes entre redes.

Logs em S3 + Athena

Para grande volume e retenção longa (logs de firewall, flow logs), o S3 com ciclo de vida é mais barato que o CloudWatch Logs. Logs do Network Firewall podem ir ao S3 pelo Data Firehose, mantendo só métricas no CloudWatch.

CloudTrail + EventBridge para mudanças de rede

Uma regra do EventBridge sobre eventos do CloudTrail, como AuthorizeSecurityGroupIngress, notifica por SNS em tempo quase real. Snapshots periódicos do Config não garantem detecção imediata.

Padronização multi-conta da telemetria

CloudFormation StackSets com implantação automática na organização criam flow logs, alarmes e dashboards em todas as contas e regiões, inclusive novas. Control Tower com StackSets direcionados às OUs dá distribuição automática e versionada.

Amazon Managed Grafana

Painel central quando o requisito pede várias fontes (Managed Prometheus, CloudWatch, OpenSearch, X-Ray) e acesso por SSO por pasta, sem depender do CloudWatch como único backend.

Macetes para memorizar

💡 As três ferramentas Monitor

Network Monitor = híbrido sem agente; Flow Monitor = fluxo entre instâncias com agente; Internet Monitor = usuário na internet.

💡 Rede da AWS x meus fluxos

A AWS está lenta? Infrastructure Performance. Eu estou lento? Network Flow Monitor.

💡 Quem registra o quê

CloudWatch mede, Flow Logs contam fluxos, CloudTrail conta APIs, Config conta configuração.

💡 Caminho

Reachability vê a configuração do caminho; Route Analyzer vê as rotas do TGW; nenhum mede tempo.

Onde guardar logs

Muito log e muito tempo: S3 + Athena. Alarme rápido: CloudWatch.

Multi-conta

Ver tudo de uma conta: cross-account observability. Criar tudo em todas: StackSets com auto-deploy.

Tabela de memorização: não confunda

Quando é...	...e quando é
CloudWatch Network Monitor Latência e perda em caminhos híbridos até o on-premises, sem agentes.	**CloudWatch Network Flow Monitor** Perda e RTT por fluxo entre instâncias e VPCs dentro da AWS, com agente nas instâncias.
Infrastructure Performance Saber se a rede da AWS entre regiões ou AZs teve aumento de latência, sem instalar nada.	**Network Flow Monitor** Saber se os meus fluxos entre workloads estão lentos ou perdendo pacotes.
VPC Reachability Analyzer Caminho entre ENIs de origem e destino considerando rotas, security groups e NACLs.	**Network Manager Route Analyzer** Validar o caminho efetivo pelas tabelas do Transit Gateway na global network.
VPC Flow Logs Visibilidade por VPC, sub-rede ou ENI, inclusive tráfego interno da VPC.	**Transit Gateway Flow Logs** Visão central do tráfego entre VPCs, VPNs e Direct Connect que passa pelo Transit Gateway.
VPC Flow Logs Metadados de fluxo em escala para auditoria, segurança e análise de padrões.	**Traffic Mirroring** Payload completo para inspeção profunda ou forense em interfaces críticas.
CloudWatch Synthetics Testar ativamente um endpoint HTTP ou API, interno ou externo, e alarmar por latência.	**CloudWatch Internet Monitor** Ver o desempenho real dos usuários na internet chegando às aplicações na AWS, por localização.

Números que caem

Item	Valor
Retenção das métricas no CloudWatch	**15 meses**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar CloudTrail para medir latência, perda de pacotes ou volume de tráfego.
Como não cair: CloudTrail registra chamadas de API do plano de controle, não o plano de dados.

⚠ **Alerta de prova:** Usar AWS Config ou o agregador como fonte de métricas de desempenho.
Como não cair: Config registra configuração e conformidade. Métricas e logs operacionais são CloudWatch.

⚠ **Alerta de prova:** Calcular latência ou perda a partir de VPC Flow Logs.
Como não cair: Flow Logs não medem latência nem perda. Use Network Monitor, Network Flow Monitor ou Synthetics.

⚠ **Alerta de prova:** Usar Reachability Analyzer para monitoramento contínuo de RTT.
Como não cair: Ele verifica configuração em um ponto no tempo; não mede desempenho.

⚠ **Alerta de prova:** Instalar tcpdump ou agente SNMP no Transit Gateway.
Como não cair: É serviço gerenciado, sem sistema operacional nem SNMP. Use métricas nativas e TGW Flow Logs.

⚠ **Alerta de prova:** Escolher Internet Monitor para rotas BGP ou latência até o data center.
Como não cair: Internet Monitor é usuários na internet para aplicações AWS. Híbrido é Network Monitor; eventos BGP, Network Manager.

⚠ **Alerta de prova:** Achar que VPC Flow Logs geram métricas de bytes e pacotes diretamente no CloudWatch.
Como não cair: São logs; precisam de metric filters ou processamento. Para tráfego por instância, use NetworkIn e NetworkOut.

⚠ **Alerta de prova:** Enviar todos os flow logs ao CloudWatch Logs com retenção de um ano.
Como não cair: Para volume grande e retenção longa, S3 com Athena e ciclo de vida é a escolha econômica.

⚠ **Alerta de prova:** Usar Traffic Mirroring para monitoramento contínuo de capacidade.
Como não cair: Mirroring duplica pacotes e custa caro; capacidade se vê com métricas nativas e flow logs.

⚠ **Alerta de prova:** Escolher CloudWatch Agent quando o enunciado proíbe agentes.
Como não cair: Sem agente: métricas nativas do EC2, Transit Gateway, VPN e Network Monitor. O agente só entra para limites do ENA ou métricas de sistema.

⚠ **Alerta de prova:** Usar X-Ray para investigar latência da rede.
Como não cair: X-Ray rastreia requisições de aplicação e exige instrumentar o código; não mede a rede.

⚠ **Alerta de prova:** Confiar em uma telemetria de saltos do Cloud WAN entre VPCs.
Como não cair: Esse recurso não existe. Desempenho por fluxo é Network Flow Monitor; Cloud WAN e Transit Gateway têm métricas no CloudWatch e eventos no Network Manager.

⚠ **Alerta de prova:** Usar Synthetics para medir perda de pacotes até o on-premises.
Como não cair: Synthetics testa endpoints e APIs de aplicação. Perda entre redes é Network Monitor.

Como cai na prova

📝 **Como cai:** Requisito de medir latência e perda com o menor esforço e sem agentes, em ambiente híbrido ou multi-VPC.
Como resolver: Descarte de cara CloudTrail, Config e Flow Logs. Veja onde está o caminho: até on-premises (Network Monitor), entre instâncias (Network Flow Monitor, com agente), usuários na internet (Internet Monitor), rede da AWS (Infrastructure Performance).

📝 **Como cai:** Troubleshooting de conectividade entre VPCs por um Transit Gateway em várias contas.
Como resolver: Para caminho e bloqueio de configuração, Reachability Analyzer com análise entre contas. Para rotas efetivas na topologia, Route Analyzer do Network Manager. Para ver o tráfego real, flow logs.

📝 **Como cai:** Centralizar observabilidade de dezenas de contas sem código customizado.
Como resolver: CloudWatch cross-account observability com uma monitoring account, flow logs entregues na conta central e StackSets para padronizar alarmes e dashboards. Rejeite Lambda em cada conta, exportação em CSV e Config como fonte de métricas.

📝 **Como cai:** Retenção longa de logs de rede com custo controlado e consultas.
Como resolver: VPC e Transit Gateway Flow Logs em bucket S3 central, particionados, consultados pelo Athena; CloudWatch apenas para métricas e alarmes.

📝 **Como cai:** Alarmar queda de túnel VPN ou descarte no Transit Gateway.
Como resolver: Use a métrica nativa (TunnelState, PacketDropCountNoRoute) com alarme do CloudWatch e EventBridge para SNS ou Automation. Rejeite agentes SNMP e scripts de ping.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
latência e perda até o on-premises, Direct Connect ou VPN, sem agentes	**CloudWatch Network Monitor**

RTT e perda por fluxo entre instâncias ou VPCs, localizar o trecho degradado	**CloudWatch Network Flow Monitor**
usuários na internet, desempenho por localização	**CloudWatch Internet Monitor**
a rede da AWS entre AZs ou regiões teve latência maior, sem instalar nada	**Infrastructure Performance do Network Manager**
por que A não alcança B, caminho salto a salto, sem agentes	**VPC Reachability Analyzer**
topologia global, eventos de rotas BGP, Transit Gateways e SD-WAN	**Network Manager com global network e EventBridge**
pacotes descartados por falta de rota no Transit Gateway	**PacketDropCountNoRoute e PacketDropCountBlackhole**
túnel VPN caiu, alarme de UP/DOWN	**Métrica TunnelState com alarme e EventBridge para SNS**
monitoring account, source accounts, sem copiar dados	**CloudWatch cross-account observability**
retenção de um ano, consultas SQL, custo baixo	**Flow logs no S3 com Athena e particionamento**
payload, inspeção profunda de pacotes	**Traffic Mirroring**
alerta imediato quando alguém alterar security group	**EventBridge sobre eventos do CloudTrail com SNS**
latência de um endpoint HTTP acima de um limite por alguns minutos	**Canary do CloudWatch Synthetics com alarme**
tráfego por instância sem agente, 15 meses de histórico	**Métricas nativas do EC2 (NetworkIn, NetworkOut)**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- CloudTrail, Config e Flow Logs nunca medem latência ou perda de pacotes.
- Antes de qualquer solução customizada, procure a métrica nativa do CloudWatch do serviço.
- Volume grande e retenção longa de logs: S3 + Athena.

Essenciais para a prova (checklist)

☐ Sei qual ferramenta CloudWatch usar para caminhos híbridos, fluxos entre instâncias e usuários na internet.

☐ Sei o que o Reachability Analyzer analisa e o que ele não mede.

☐ Sei o que o Network Manager oferece: global network, Route Analyzer, Infrastructure Performance e eventos.

☐ Sei as métricas nativas do Transit Gateway e da VPN usadas em alarmes.

- ☐ Sei por que VPC Flow Logs não servem para latência e como transformá-los em métricas.
- ☐ Sei quando usar Transit Gateway Flow Logs em vez de VPC Flow Logs.
- ☐ Sei montar observabilidade multi-conta com monitoring account e source accounts.
- ☐ Sei escolher entre CloudWatch Logs e S3 + Athena por custo e retenção.
- ☐ Sei quando o Traffic Mirroring se justifica.

Questões de revisão do capítulo

R3.1 · Network Management and Operation

Você está projetando uma solução de observabilidade de rede em uma arquitetura híbrida que utiliza múltiplas VPCs, Direct Connect e VPNs. A equipe de segurança exige visibilidade detalhada do tráfego, correlação com métricas de desempenho e a capacidade de inspecionar fluxos específicos para investigação de incidentes. Qual combinação de serviços e recursos da AWS atende melhor a esses requisitos, seguindo as práticas recomendadas de observabilidade de rede?

A. Usar o AWS Config para rastrear mudanças nos recursos de rede e relatórios periódicos para achar padrões de tráfego e incidentes
B. Ativar só VPC Flow Logs e exportá-los ao S3, com consultas ad hoc em ferramentas externas para qualquer análise ou correlação
C. Usar o CloudTrail para registrar as chamadas de API de rede, já que ele dá visibilidade suficiente do tráfego de dados das VPCs
D. Usar flow logs das VPCs no CloudWatch Logs com filtros de métricas e alarmes, e Traffic Mirroring seletivo para enviar cópias de fluxos suspeitos a appliances

R3.2 · Network Management and Operation

Uma empresa está migrando diversas cargas de trabalho para a AWS e deseja padronizar a coleta de métricas de rede (latência, perda de pacotes, throughput) e a detecção de anomalias em todas as contas e regiões. A equipe de arquitetura quer uma solução gerenciada, com o mínimo de sobrecarga operacional, que permita aplicar políticas de monitoramento centralizadas e gerar alarmes automaticamente quando o desempenho da rede ficar abaixo de determinados limiares. Qual abordagem atende melhor a esses requisitos?

A. Utilizar AWS CloudTrail para registrar chamadas de API de rede e configurar alarmes no Amazon CloudWatch Logs Insights para latência e perda de pacotes.
B. Implantar instâncias EC2 dedicadas rodando ferramentas de monitoramento de rede de terceiros em cada VPC e consolidar os dados em um banco de dados central.
C. Configurar VPC Flow Logs em todas as VPCs, exportar para Amazon S3 e criar consultas agendadas no Amazon Athena para detectar anomalias de rede.
D. Usar o CloudWatch Internet Monitor com um monitor por aplicação exposta na internet, alarmes do CloudWatch sobre desempenho e disponibilidade e visão por local dos usuários

R3.3 · Network Management and Operation

Você está operando um ambiente multi-contas em AWS Organizations com dezenas de VPCs conectadas a um AWS Transit Gateway. O time de operações precisa de visibilidade centralizada e em tempo quase real sobre o estado de conectividade (reachability) entre VPCs, rotas aprendidas e possíveis quedas de anexos. Qual solução gerenciada da AWS é mais adequada para diagnosticar e monitorar continuamente a conectividade de rede nesse cenário, com integração nativa a CloudWatch e EventBridge?

A. AWS Network Manager com uma global network, o Transit Gateway registrado e o Route Analyzer
B. AWS CloudTrail com logs de chamadas de API de EC2 e VPC, analisados via AWS Athena
C. AWS Systems Manager Automation para executar scripts periódicos de teste de ping entre instâncias nas VPCs
D. AWS Config com regras gerenciadas para verificar conformidade de rotas em route tables

R3.4 · Network Management and Operation

Uma equipe de SRE precisa padronizar a coleta de métricas de rede (latência, perda de pacotes, throughput) entre múltiplas VPCs em diferentes contas AWS e Regiões, com o menor esforço operacional possível. As métricas devem ser integradas ao Amazon CloudWatch para geração de alarmes centralizados e dashboards. Qual abordagem é MAIS adequada para atender a esse requisito?

A. Configurar CloudWatch Internet Monitor para todos os endpoints acessados a partir das VPCs, e usar as métricas geradas (como performance e disponibilidade) para alarmes e dashboards centralizados em uma única conta.
B. Habilitar o VPC Flow Logs em todas as VPCs, exportar os logs para o CloudWatch Logs e usar métricas de log (metric filters) para derivar latência fim a fim, perda de pacotes e throughput entre workloads.
C. Ativar AWS Network Manager com monitoramento de Transit Gateways entre contas e Regiões, e usar as métricas do CloudWatch associadas aos Transit Gateways para inferir latência detalhada e perda de pacotes entre todas as instâncias EC2.
D. Utilizar Reachability Analyzer em cada VPC, exportar os resultados para Amazon S3 e criar uma solução customizada que leia esses arquivos e envie métricas para o CloudWatch via scripts agendados em instâncias EC2.

Respostas comentadas

R3.1. D) Usar flow logs das VPCs no CloudWatch Logs com filtros de métricas e alarmes, e Traffic Mirroring seletivo para enviar cópias de fluxos suspeitos a appliances

Por quê: Esta alternativa é a mais adequada porque combina diferentes camadas de observabilidade de rede, alinhadas com as práticas recomendadas da AWS: - VPC Flow Logs fornecem visibilidade sobre os fluxos de tráfego de rede em nível de interface, sub-rede ou VPC, permitindo identificar padrões, falhas de conexão e possíveis comportamentos anômalos.

✗ A) Incorreta. O Config registra configuração, não tráfego.
✗ B) Incorreta. Sem correlação com métricas nem inspeção de pacotes, requisitos do cenário.
✗ C) Incorreta. O CloudTrail registra chamadas de API, não o tráfego de dados.

R3.2. D) Usar o CloudWatch Internet Monitor com um monitor por aplicação exposta na internet, alarmes do CloudWatch sobre desempenho e disponibilidade e visão por local dos usuários

Por quê: Esta alternativa é a mais adequada porque o AWS CloudWatch Internet Monitor é um serviço gerenciado projetado especificamente para monitorar desempenho e disponibilidade de aplicações acessadas pela internet, com métricas como latência, perda de pacotes e impacto em usuários. Ele agrega dados por região e por aplicação, permite centralizar a observabilidade em múltiplas contas e regiões por meio de contas de monitoramento centralizadas, e integra nativamente com alarmes do Amazon CloudWatch.

✗ A) Incorreta. AWS CloudTrail registra chamadas de API (quem fez o quê, quando e de onde), e não métricas de rede como latência, jitter ou perda de pacotes.

✗ B) Incorreta. Ferramentas de terceiros em instâncias EC2 podem fornecer métricas de rede, mas exigem implantação, manutenção, escalabilidade e atualização contínuas, além de gestão de licenças.

✗ C) Incorreta. VPC Flow Logs fornecem informações de tráfego (aceito, rejeitado, bytes, pacotes), mas não medem diretamente latência ou perda de pacotes.

> **Dica de prova:** Quando o enunciado enfatizar monitoramento de desempenho de aplicações expostas à internet, com foco em latência, perda de pacotes e impacto em usuários, pense em CloudWatch Internet Monitor.

R3.3. A) AWS Network Manager com uma global network, o Transit Gateway registrado e o Route Analyzer

Por quê: Esta alternativa é a mais adequada porque o AWS Network Manager, em conjunto com o Global Network, foi projetado especificamente para gestão e operação de redes em larga escala. Ao anexar o AWS Transit Gateway ao Global Network e habilitar o Network Connectivity Analyzer, você obtém: - Visibilidade centralizada de conectividade entre VPCs, on-premises e outros domínios. - Análise de reachability baseada em rotas, anexos e políticas, não apenas em testes de ping.

✗ B) Incorreta. CloudTrail + Athena ajudam em auditoria e análise de histórico de chamadas de API, mas não fornecem monitoramento contínuo de reachability, nem visão de topologia ou análise de rotas em tempo quase real.

✗ C) Incorreta. Systems Manager Automation pode rodar scripts de ping entre instâncias, mas isso é manual, pouco escalável e frágil.

✗ D) Incorreta. AWS Config verifica conformidade de recursos e pode checar se certas rotas existem, mas não faz teste de conectividade ponta a ponta, nem oferece correlação operacional entre anexos, rotas e estado da rede de forma centralizada.

> **Dica de prova:** Para questões de operação de rede em ambientes com AWS Transit Gateway, pense em AWS Network Manager + Global Network quando o enunciado falar de: multi-conta, multi-região, visibilidade topológica, monitoramento contínuo de conectividade e integração com CloudWatch/EventBridge.

R3.4. A) Configurar CloudWatch Internet Monitor para todos os endpoints acessados a partir das VPCs, e usar as métricas geradas (como performance e disponibilidade) para alarmes e dashboards centralizados em uma única conta.

Por quê: Esta alternativa é a mais adequada porque o Amazon CloudWatch Internet Monitor foi projetado especificamente para monitorar a performance e disponibilidade de tráfego da sua aplicação na internet, incluindo métricas de latência e perda de pacotes, de forma gerenciada e integrada ao CloudWatch. Ele permite monitorar endpoints (como Application Load Balancers, CloudFront, API Gateway, IPs elásticos) em múltiplas Regiões e contas, centralizando a visibilidade.

✗ B) Incorreta. VPC Flow Logs fornecem informações de fluxo (aceito/negado, bytes, pacotes, portas, IPs, etc.), mas não fornecem diretamente métricas confiáveis de latência fim a fim nem de perda de pacotes entre workloads.

✗ C) Incorreta. AWS Network Manager e métricas de Transit Gateway ajudam a monitorar conectividade e estatísticas de tráfego entre VPCs e redes on-premises (bytes, pacotes, drops por motivo, etc.), mas não expõem a latência detalhada e perda de...

✗ D) Incorreta. Reachability Analyzer é uma ferramenta de verificação de caminho e análise estática de conectividade, não um serviço contínuo de monitoramento de métricas como latência e perda de pacotes.

Dica de prova: Para questões de prova envolvendo observabilidade de rede, associe: - CloudWatch Internet Monitor: performance e disponibilidade de tráfego de internet (latência, perda, eventos de performance) para endpoints públicos.

04

CAPÍTULO 4 · 24% DA PROVA

Network Security, Compliance, and Governance

Aqui eu preciso separar com precisão quem previne, quem detecta, quem corrige e quem inspeciona. A prova quase sempre traz um ambiente com dezenas de contas no AWS Organizations e pede a combinação com menor esforço operacional: SCP para bloquear o que não pode acontecer, Firewall Manager para impor WAF, security groups e Network Firewall em contas atuais e futuras, Config para detectar e remediar, CloudTrail para saber quem fez o quê. Na parte de tráfego, o padrão campeão é Transit Gateway + VPC de inspeção com appliance mode, usando Network Firewall ou Gateway Load Balancer com appliances de terceiros. Onde mais erro: escolher uma ferramenta detectiva quando o enunciado pede prevenção, ou achar que CloudTrail e Flow Logs registram coisas que não registram.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

AWS Firewall Manager

Gerencia de forma central políticas de AWS WAF, Shield Advanced, security groups e AWS Network Firewall em todas as contas da organização, incluindo contas futuras. Faz auditoria contínua e pode corrigir automaticamente recursos fora do padrão. Exige integração com AWS Organizations e trabalha junto com o AWS Config. A política precisa ter escopo na organização inteira e remediação automática ativada para cobrir contas novas.

Service Control Policy (SCP)

Guarda-corpo preventivo do AWS Organizations: define o máximo que qualquer conta pode fazer. Uma negação em SCP é definitiva, nenhuma política IAM ou permission boundary a sobrescreve. Use condições e tags para precisão, por exemplo negar ec2:CreateInternetGateway e ec2:AttachInternetGateway só na OU de desenvolvimento, ou negar AuthorizeSecurityGroupIngress com 0.0.0.0/0 nas portas 22 e 3389. SCP aplicada na raiz atinge todas as contas, inclusive produção.

AWS Config (agregador, conformance packs, remediação)

Avalia continuamente a configuração dos recursos e guarda o histórico de mudanças. Com agregador na conta de segurança ou auditoria, dá visão multi-conta; com remediação pelo Systems Manager Automation, corrige desvios. É detectivo e corretivo: não impede que o recurso inseguro seja criado, sempre existe uma janela de exposição.

AWS Control Tower

Padroniza a landing zone e aplica controles preventivos e detectivos (guardrails) às contas e OUs. É a resposta para guardrails de conta e padrões de VPC em várias contas. Não gerencia o conteúdo dos security groups; para políticas de firewall entre contas, o serviço é o Firewall Manager.

AWS CloudTrail (trail organizacional e CloudTrail Lake)

Registra chamadas de API: quem fez o quê, quando e de onde, inclusive alterações em security groups e NACLs. Trail organizacional centraliza o registro de todas as contas; CloudTrail Lake permite análise. Não registra consultas DNS nem o tráfego de dados da rede.

S3 Object Lock no modo Compliance

Torna os logs imutáveis (WORM), impedindo exclusão ou alteração mesmo por administradores. Bucket policy restritiva sozinha não garante imutabilidade. O padrão de prova é uma conta central de log archive recebendo o trail da organização, o Config e os flow logs, com bloqueio de acesso público e gravação só pelos serviços de log.

Route 53 Resolver DNS Firewall

Bloqueia consultas a domínios maliciosos ou de exfiltração em todas as VPCs, com listas de domínios gerenciadas pela AWS e ação de bloqueio, sem agentes nas instâncias. O tráfego até o Resolver da VPC não passa por security groups nem NACLs, então filtrar a porta 53 não funciona e ainda quebra a resolução. Em multi-conta: endpoints do Resolver em conta central, regras compartilhadas pelo RAM e query logging.

VPC de inspeção com Transit Gateway e appliance mode

Padrão para inspecionar leste-oeste (entre VPCs) e norte-sul (internet e on-premises) em um ponto central. As tabelas do Transit Gateway enviam o tráfego das spokes para a VPC de inspeção, e o appliance mode no attachment dela mantém os fluxos simétricos para firewalls stateful. O desenho típico usa duas tabelas: uma para as spokes e outra para a inspeção.

Gateway Load Balancer (GWLB)

Insere appliances de segurança de terceiros de forma transparente no caminho do tráfego, com escala e alta disponibilidade gerenciadas. Os GWLB endpoints viram destino das rotas (inclusive das rotas vindas do Transit Gateway). Quando o enunciado exige firewall de terceiros, o AWS Network Firewall não atende, porque é serviço gerenciado da AWS.

AWS Network Firewall

Firewall gerenciado stateful inserido por roteamento: as sub-redes privadas apontam 0.0.0.0/0 para os endpoints dele em sub-redes dedicadas. Faz inspeção avançada, inclusive de camada 7 e listas de domínios para egress. Não criptografa enlace e não se associa a listeners de ALB. Em modo apenas stateless não atende inspeção completa de saída.

MACsec no Direct Connect

Criptografia de alta banda no enlace entre o roteador do cliente e o dispositivo da AWS, sem perder desempenho com túneis IPsec. Configura-se associando a chave CKN/CAK à conexão dedicada compatível. Não existe em ENIs de instâncias nem em conexões hospedadas; nesses casos, a saída é VPN Site-to-Site com IP privado sobre o Direct Connect.

Network Access Analyzer

Gera evidência de que não existe caminho entre origens e destinos em escala, considerando rotas, security groups e NACLs, por exemplo provar que nenhum banco é alcançável a partir de um internet gateway. Difere do Reachability Analyzer, que testa um caminho específico por vez.

VPC Block Public Access

Bloqueia o tráfego de e para internet gateways em todas as VPCs, no modo bidirecional, com exclusões para VPCs ou sub-redes aprovadas (como a VPC de egress). Vale mesmo se alguém alterar rotas ou security groups, diferentemente de NACLs que os donos das contas podem mudar.

AWS Verified Access

Dá acesso a aplicações web internas sem VPN, avaliando a identidade no provedor corporativo e a postura do dispositivo a cada requisição, com trust providers e políticas por aplicação. Client VPN continua sendo VPN e não avalia o dispositivo a cada requisição.

DNSSEC no Route 53

A assinatura usa uma key-signing key (KSK) baseada em chave KMS assimétrica em us-east-1. Depois de ativar a assinatura na hosted zone, falta criar o registro DS da KSK na zona pai para estabelecer a cadeia de confiança. A chave pública fica no registro DNSKEY, criado pelo Route 53.

Políticas de chave do KMS

A key policy é a autoridade principal sobre a chave; IAM sozinho não basta se a key policy for permissiva. Condições cobradas: aws:PrincipalOrgID para limitar à organização, kms:ViaService para limitar ao serviço e aws:SourceVpce para exigir o VPC endpoint do KMS. Para compliance, prefira chave gerenciada pelo cliente com rotação automática e uso auditado no CloudTrail; security groups não controlam quem usa uma chave.

VPN Site-to-Site com certificados da AWS Private CA

Substitui a chave pré-compartilhada (PSK) por autenticação mútua baseada em certificados, com emissão e rotação automatizadas e sem PKI própria fora da AWS. Client VPN não serve para ligar redes site a site.

Systems Manager Session Manager

Acesso administrativo às instâncias sem SSH aberto e sem bastion público, com sessões registradas no S3 ou no CloudWatch Logs para auditoria. É a resposta quando o enunciado pede trilha detalhada de ações administrativas em EC2.

Macetes para memorizar

💡 Camadas de governança

SCP proíbe, Firewall Manager impõe, Config confere e conserta, CloudTrail conta quem fez.

💡 CloudTrail x Config x Flow Logs

Trail = quem mexeu; Config = como está e como ficou; Flow Logs = quem conversou com quem.

💡 Inspeção central

TGW + VPC de inspeção + appliance mode: o trio que não deixa o retorno fugir do firewall.

💡 Analyzers

Network Access Analyzer prova que NÃO existe caminho em escala; Reachability Analyzer testa UM caminho.

💡 Criptografia do Direct Connect

Dedicada: MACsec. Hospedada: VPN privada por cima do DX.

💡 DNSSEC

KSK com KMS assimétrica em us-east-1, e o DS sobe para o pai.

💡 Negação em SCP

Deny de SCP é cadeado: nem IAM nem permission boundary abrem. Por isso, escolha bem a OU.

Tabela de memorização: não confunda

Quando é...	...e quando é
SCP Bloquear de forma preventiva o que nenhuma conta pode fazer: criar internet gateway, peering fora da conta de segurança, rota 0.0.0.0/0 sem passar pelo NAT aprovado.	**AWS Firewall Manager** Impor e manter o conteúdo das regras: Web ACLs do WAF, security groups e Network Firewall em contas atuais e futuras, com auditoria e correção automática.
AWS Config Estado e histórico de configuração dos recursos, avaliação de conformidade contínua e remediação automática.	**AWS CloudTrail** Trilha de auditoria de chamadas de API: quem alterou o security group, quando e de onde.
Network Access Analyzer Provar em escala que não existe caminho, por exemplo de internet gateways até os bancos em todas as VPCs.	**VPC Reachability Analyzer** Diagnosticar um caminho específico entre uma origem e um destino.
MACsec Conexão Direct Connect dedicada compatível, criptografia de alta banda sem túneis IPsec.	**VPN com IP privado sobre Direct Connect** Conexão hospedada ou sem suporte a MACsec, mantendo o tráfego fora da internet e terminando no Transit Gateway.
AWS Control Tower Guardrails de conta, landing zone padronizada e padrões de VPC e sub-redes nas contas.	**AWS Firewall Manager** Políticas de firewall (WAF, security groups, Network Firewall) aplicadas entre contas.
AWS Network Firewall Firewall gerenciado pela AWS, com regras stateful e listas de domínios, em VPC de inspeção ou de egress.	**Gateway Load Balancer com appliances** O enunciado exige firewall ou NGFW de terceiros, inspeção TLS por appliances ou escala transparente de appliances.
AWS WAF Regras de camada 7 em ALB, API Gateway ou CloudFront, inclusive regras baseadas em IP para tráfego HTTP/HTTPS.	**AWS Shield Advanced** Proteção contra DDoS; não substitui as regras de camada 7 do WAF.

Números que caem

Item	Valor
Portas que a SCP costuma negar para 0.0.0.0/0 em security groups	**22 (SSH) e 3389 (RDP)**
Região da chave KMS assimétrica da KSK do DNSSEC no Route 53	**us-east-1**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar CloudTrail para auditar consultas DNS.
Como não cair: CloudTrail registra chamadas de API, não consultas DNS. Para DNS: Resolver query logging e DNS Firewall.

⚠ **Alerta de prova:** Escolher AWS Config com remediação quando o enunciado pede impedir a criação do recurso.
Como não cair: Config só detecta e corrige depois, com janela de exposição. Prevenção em todas as contas é SCP.

⚠ **Alerta de prova:** Aplicar a SCP de negação na raiz da organização para bloquear só desenvolvimento.
Como não cair: Negação na raiz atinge todas as contas, inclusive produção. Mova desenvolvimento para uma OU própria e anexe a SCP a ela.

⚠ **Alerta de prova:** Criar políticas IAM restritivas em cada conta como guarda-corpo.
Como não cair: Administradores locais podem alterá-las. Guarda-corpo organizacional é SCP.

⚠ **Alerta de prova:** Bloquear a porta 53 em security groups ou NACLs para filtrar domínios maliciosos.
Como não cair: O tráfego ao Resolver da VPC não passa por SGs nem NACLs, e bloquear a porta quebraria toda a resolução. Use DNS Firewall.

⚠ **Alerta de prova:** Usar PrivateLink ou VPC peering em malha para forçar inspeção entre VPCs.
Como não cair: PrivateLink expõe serviços, não roteia tráfego geral; peering não é transitivo e cresce em N*(N-1)/2 conexões. Inspeção central é Transit Gateway + VPC de inspeção.

⚠ **Alerta de prova:** Ativar MACsec nas ENIs das instâncias ou na conexão Direct Connect hospedada.
Como não cair: MACsec só existe em conexões Direct Connect dedicadas compatíveis. Sem MACsec, VPN com IP privado sobre o Direct Connect.

⚠ **Alerta de prova:** Achar que VPC Flow Logs mostram quem alterou um security group.
Como não cair: Flow Logs registram tráfego (IP, porta, ação). Mudança de configuração com autoria é CloudTrail.

⚠ **Alerta de prova:** Proteger logs de auditoria só com bucket policy que nega exclusão.
Como não cair: Administradores com permissão suficiente ainda apagam. Imutabilidade exige S3 Object Lock no modo Compliance, em conta central.

⚠ **Alerta de prova:** Trocar o WAF pelo Shield Advanced para regras de aplicação.
Como não cair: Shield Advanced é proteção DDoS. Regras de camada 7 e por IP em ALB são do WAF, distribuído pelo Firewall Manager.

⚠ **Alerta de prova:** Usar chaves gerenciadas pela AWS em cenário de compliance com controle central de chaves.
Como não cair: Escolha chave gerenciada pelo cliente, com rotação automática, key policy com separação de funções e uso auditado no CloudTrail.

⚠ **Alerta de prova:** Ativar validação DNSSEC no Route 53 Resolver para completar a cadeia de confiança do domínio público.
Como não cair: Isso só afeta as VPCs da empresa. Para os resolvers da internet, crie o registro DS da KSK na zona pai.

⚠ **Alerta de prova:** Usar Reachability Analyzer para provar que nenhum banco é alcançável pela internet em toda a conta.
Como não cair: Ele testa um caminho por vez. Ausência de caminho em escala é Network Access Analyzer.

⚠ **Alerta de prova:** Escolher Network Firewall quando o requisito diz firewall de terceiros.
Como não cair: Network Firewall é serviço da AWS. Appliance de terceiros com escala: Gateway Load Balancer.

Como cai na prova

📝 **Como cai:** Organização com muitas contas pede padronizar regras de segurança, incluindo contas futuras, com o menor esforço operacional.
Como resolver: Identifique o verbo: impor conteúdo de regras (Firewall Manager), proibir ações (SCP) ou detectar desvios (Config). Descarte Lambda, scripts e configuração conta a conta. Confira se a política cobre a organização inteira com remediação automática.

📝 **Como cai:** Todo tráfego entre VPCs, on-premises e internet deve passar por inspeção central, com auditoria.
Como resolver: Monte Transit Gateway como hub, VPC de inspeção com Network Firewall ou GWLB e appliances, tabelas de rotas forçando o caminho e appliance mode. Elimine peering em malha, PrivateLink e firewall em cada VPC.

📝 **Como cai:** Requisito de auditoria e logs que nem administradores podem apagar.
Como resolver: CloudTrail organizacional e flow logs entregues em bucket de conta central, com Object Lock no modo Compliance. Descarte opções só com bucket policy, CloudWatch Logs isolado ou buckets em cada conta.

📝 **Como cai:** Bloquear uma ação só para um grupo de contas, mantendo as demais livres.
Como resolver: Coloque as contas afetadas em uma OU e anexe a SCP de negação a ela. Rejeite SCP na raiz, SCP conta a conta e SCP em modo de auditoria com Config.

📝 **Como cai:** Escolher entre serviços parecidos de segurança (GuardDuty, Security Hub, Config, Firewall Manager).
Como resolver: GuardDuty detecta ameaças; Security Hub agrega achados; Config avalia configuração; Firewall Manager aplica políticas de firewall. Só o último cria e aplica regras entre contas.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
dezenas de contas, contas atuais e futuras, correção automática de WAF ou security groups	**AWS Firewall Manager com AWS Organizations**
impedir em todas as contas, nenhuma conta pode, mesmo administradores	**SCP na OU correta**
quem fez o quê, quando e de onde	**AWS CloudTrail (trail organizacional)**
logs imutáveis, WORM, não podem ser apagados por administradores	**S3 Object Lock modo Compliance em conta de log archive**
bloquear domínios maliciosos, exfiltração por DNS, sem agentes	**Route 53 Resolver DNS Firewall**
inspeção leste-oeste centralizada, VPCs no Transit Gateway, firewall stateful	**VPC de inspeção + appliance mode no attachment**
appliances de terceiros, escala e alta disponibilidade, transparente	**Gateway Load Balancer e GWLB endpoints**
criptografar Direct Connect dedicado sem perder banda	**MACsec com CKN/CAK**
provar que não existe caminho da internet até os bancos em todas as VPCs	**Network Access Analyzer**
bloquear internet em todas as VPCs com poucas exceções aprovadas	**VPC Block Public Access bidirecional com exclusões**
aplicações internas sem VPN, identidade e postura do dispositivo a cada requisição	**AWS Verified Access**
DNSSEC ativado, resolvers ainda não validam	**Registro DS da KSK na zona pai**
acesso administrativo sem SSH, sessões auditadas	**Systems Manager Session Manager**
VPN site a site com autenticação por certificados e rotação automática	**Site-to-Site VPN com AWS Private CA**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Prevenir é SCP; Config detecta e corrige depois, e Security Hub só agrega achados.
- Firewall Manager é a resposta para políticas de WAF, security groups e Network Firewall em contas atuais e futuras.
- CloudTrail não registra consultas DNS nem tráfego; Flow Logs não registram mudanças de configuração.
- Inspeção central com Transit Gateway exige appliance mode no attachment da VPC de inspeção.
- Logs imutáveis só com S3 Object Lock no modo Compliance.

Essenciais para a prova (checklist)

- ☐ Sei quando usar SCP, Firewall Manager, Config, Control Tower, Security Hub e GuardDuty.
- ☐ Sei montar a inspeção leste-oeste e norte-sul com Transit Gateway, VPC de inspeção e appliance mode.
- ☐ Sei diferenciar AWS Network Firewall de Gateway Load Balancer com appliances de terceiros.
- ☐ Sei por que filtrar a porta 53 não bloqueia domínios e quando usar DNS Firewall.
- ☐ Sei as opções para criptografar Direct Connect dedicado e hospedado.
- ☐ Sei montar uma conta de log archive com trail organizacional e Object Lock.
- ☐ Sei quais condições de key policy restringem uso por organização, serviço e VPC endpoint.
- ☐ Sei o que falta para o DNSSEC funcionar depois de ativar a assinatura.
- ☐ Sei quando usar Network Access Analyzer e quando usar Reachability Analyzer.
- ☐ Sei aplicar uma SCP só às contas de uma OU sem afetar produção.

Questões de revisão do capítulo

R4.1 · Network Security, Compliance, and Governance

Uma organização sob requisitos rígidos de compliance precisa garantir que o tráfego entre VPCs de regiões diferentes seja criptografado em trânsito e não passe pela internet, com a menor interferência possível nas aplicações. Cada região já usa um AWS Transit Gateway. Qual abordagem atende com o menor impacto?

A. Implementar Appliance de firewall de terceiros em modo proxy TLS em cada VPC, forçando o tráfego inter-VPC a passar por esses appliances para criptografia.
B. Configurar VPNs IPsec site-to-site entre cada par de VPCs, substituindo a conectividade via AWS Transit Gateway
C. Ativar a opção de criptografia em trânsito (MACsec) diretamente nas interfaces de rede elásticas (ENIs) das instâncias EC2 em todas as VPCs.
D. Criar um peering entre os Transit Gateways das regiões, cujo tráfego segue pela rede global da AWS com criptografia automática

R4.2 · Network Security, Compliance, and Governance

Uma empresa de e-commerce que processa dados de titulares de cartão em múltiplas contas AWS precisa comprovar conformidade com PCI DSS. A equipe de segurança quer centralizar a coleta de CloudTrail, VPC Flow Logs e logs de segurança em uma única conta, garantindo que os logs sejam imutáveis, com retenção de longo prazo e protegidos contra exclusão ou alteração por administradores das contas membro. Qual combinação de ações atende melhor aos requisitos de conformidade e governança com o menor esforço operacional?

A. Habilitar AWS Config nas contas para registrar as mudanças de configuração, exportar os snapshots de configuração para um bucket S3 central e usar Amazon GuardDuty para monitorar tráfego suspeito, mantendo os findings em CloudWatch Logs por, no mínimo, sete anos.
B. Criar um bucket S3 em cada conta membro, habilitar CloudTrail e VPC Flow Logs para gravar nesses buckets locais e usar AWS Backup para copiar diariamente os logs para um bucket S3 na conta central, com criptografia por SSE-S3 e ciclo de vida para arquivamento em S3 Glacier Deep Archive.
C. Criar um bucket S3 na conta central de segurança, habilitar AWS CloudTrail nas contas membro com destino nesse bucket, habilitar VPC Flow Logs apontando para o mesmo bucket e aplicar uma política de bucket que negue exclusão de objetos para os usuários, exceto o root da conta central.
D. Usar trail organizacional em um bucket S3 central com Object Lock no modo Compliance, CloudTrail Lake para análise e VPC Flow Logs entregues na conta central

R4.3 · Network Security, Compliance, and Governance

Uma equipe de segurança precisa garantir que todo o tráfego entre workloads em uma VPC e serviços da AWS (como Amazon S3 e Amazon DynamoDB) ocorra de forma privada, sem exposição à internet pública, e que as conexões usem automaticamente TLS gerenciado pela AWS, atendendo requisitos de conformidade. Além disso, a equipe quer evitar o gerenciamento manual de certificados nos servidores de aplicação. Qual combinação de soluções atende melhor a esses requisitos?

A. Criar um AWS Site-to-Site VPN entre a VPC e a internet pública, utilizando túneis IPsec para proteger o tráfego, e instalar certificados TLS em cada instância à mão.
B. Usar interface endpoints do PrivateLink para S3 e DynamoDB na VPC e o ACM nos ALBs para terminar TLS nas aplicações
C. Habilitar NAT Gateways nas sub-redes privadas e configurar regras de rota para enviar o tráfego de S3 e DynamoDB pela internet, usando certificados autoassinados nas instâncias.
D. Usar gateways de internet para as sub-redes, permitir só tráfego HTTPS (porta 443) em security groups.

R4.4 · Network Security, Compliance, and Governance

Um auditor de compliance exigiu que todo tráfego entre workloads sensíveis em uma VPC da AWS e um datacenter on-premises seja inspecionado por um appliance de segurança de terceiros, com a capacidade de registrar metadados de fluxo para fins de auditoria. A conexão atual é feita por AWS Direct Connect com uma private virtual interface (VIF) ligada a um Virtual Private Gateway (VGW). O time de redes precisa atender ao requisito com o mínimo de impacto na disponibilidade e seguindo boas práticas de segurança. Qual é a abordagem MAIS adequada?

A. Manter o VGW e Direct Connect como estão, criar um AWS Network Firewall em sub-redes dedicadas na VPC e anunciar rotas mais específicas para forçar o tráfego on-premises a passar pelo firewall.
B. Configurar um VPN site-to-site sobre o Direct Connect usando o VGW, desativar o BGP dinâmico e usar apenas rotas estáticas apontando para uma instância NAT que encaminha o tráfego para o appliance de segurança antes de seguir para on-premises.
C. Substituir o Virtual Private Gateway por um AWS PrivateLink endpoint para o datacenter on-premises, e usar o PrivateLink como ponto de inspeção.
D. Usar um Transit Gateway com a VPC e o Direct Connect gateway anexados e uma VPC de inspeção centralizada, com rotas que forçam o tráfego por ela

Respostas comentadas

R4.1. D) Criar um peering entre os Transit Gateways das regiões, cujo tráfego segue pela rede global da AWS com criptografia automática

Por quê: O tráfego entre regiões pelo Transit Gateway peering segue pela rede global da AWS, nunca pela internet pública, e é criptografado. Isso atende ao requisito sem alterar as aplicações nem criar túneis.

✗ A) Incorreta. Proxies TLS em cada VPC adicionam complexidade e mudam o caminho das aplicações.

✗ B) Incorreta. Cria uma malha de túneis difícil de operar, limitada em banda, e desmonta o Transit Gateway.

✗ C) Incorreta. MACsec existe em conexões Direct Connect dedicadas, não em ENIs de instâncias.

> **Dica de prova:** Criptografia entre regiões sem mexer nas aplicações: Transit Gateway peering ou VPC peering entre regiões.

R4.2. D) Usar trail organizacional em um bucket S3 central com Object Lock no modo Compliance, CloudTrail Lake para análise e VPC Flow Logs entregues na conta central

Por quê: Esta alternativa é a mais adequada porque combina centralização, governança em nível de organização e imutabilidade dos logs, aspectos críticos para PCI DSS. O uso de AWS Organizations com um Organization Trail garante que todas as contas membro tenham CloudTrail habilitado de forma consistente e enviando para um bucket S3 na conta central, reduzindo risco de desvio de configuração. O AWS CloudTrail Lake oferece capacidade de análise centralizada e retenção flexível.

✗ A) Incorreta. AWS Config e GuardDuty são serviços importantes de governança e detecção de ameaças, mas não substituem CloudTrail e VPC Flow Logs como trilhas de auditoria primárias de API e tráfego de rede.

✗ B) Incorreta. Mantém logs inicialmente distribuídos em diferentes contas, o que aumenta a superfície de risco e a complexidade de auditoria.

✗ C) Incorreta. Usa apenas política de bucket S3 para restringir exclusão, mas sem S3 Object Lock em modo Compliance os administradores com permissões suficientes ainda podem alterar políticas ou remover a proteção.

> **Dica de prova:** Para requisitos de conformidade que pedem logs imutáveis (WORM), lembre-se: S3 Object Lock em modo Compliance é o mecanismo recomendado; políticas de bucket sozinhas não são suficientes.

R4.3. B) Usar interface endpoints do PrivateLink para S3 e DynamoDB na VPC e o ACM nos ALBs para terminar TLS nas aplicações

Por quê: Esta alternativa é a correta porque combina isolamento de rede com criptografia gerenciada. Os endpoints de interface (AWS PrivateLink) permitem acesso privado a serviços da AWS a partir da VPC, sem utilizar IPs públicos ou internet, atendendo requisitos de segurança e compliance.

✗ A) Incorreta. Site-to-Site VPN é projetada para conectar redes on-premises a VPCs, não para proteger tráfego entre VPC e serviços públicos da AWS. Ainda exige gerenciamento manual de certificados em cada instância, o que a questão quer evitar.

✗ C) Incorreta. Utiliza NAT Gateway e internet pública para acessar S3 e DynamoDB, o que não atende ao requisito de evitar exposição à internet.

✗ D) Incorreta. Depende de exposição via internet pública por meio de internet gateways e apenas restringe portas. Isso não garante acesso privado aos serviços da AWS e não resolve o requisito de gerenciamento centralizado de TLS e certificados.

> **Dica de prova:** Quando o enunciado mencionar 'acesso privado a serviços da AWS sem passar pela internet' pense em VPC endpoints (interface ou gateway). Quando a questão falar em 'evitar gerenciamento manual de certificados TLS' e 'renovação automática', a combinação típica é usar ACM com ALB/NLB ou CloudFront.

R4.4. D) Usar um Transit Gateway com a VPC e o Direct Connect gateway anexados e uma VPC de inspeção centralizada, com rotas que forçam o tráfego por ela

Por quê: Esta alternativa é a mais adequada porque segue o padrão de referência da AWS para inspeção centralizada de tráfego usando AWS Transit Gateway. Ao anexar tanto a VPC quanto o Direct Connect (via Direct Connect Gateway) ao Transit Gateway, é possível criar um 'VPC de inspeção' (inspection VPC) com appliances de segurança de terceiros e controlar de forma escalável, resiliente e simétrica o roteamento do tráfego entre on-premises e workloads sensíveis.

✗ A) Incorreta. O AWS Network Firewall protege tráfego dentro/para fora da VPC, mas não é automaticamente um ponto de inspeção inline entre a VPC e o VGW de Direct Connect.

✗ B) Incorreta. Criar VPN sobre Direct Connect e desativar BGP dinâmico aumenta complexidade operacional, reduz resiliência (perda de failover dinâmico) e usa uma instância NAT como ponto de passagem, o que não é uma boa prática para inspeção...

✗ C) Incorreta. AWS PrivateLink não é projetado para substituir o Virtual Private Gateway nem para encaminhar tráfego roteado genérico para um datacenter on-premises. PrivateLink publica serviços específicos como endpoints;

Dica de prova: Para cenários de compliance que exigem inspeção centralizada de tráfego entre múltiplas VPCs e ambientes on-premises, lembre-se: Transit Gateway + VPC de inspeção/appliance de terceiros é o padrão recomendado, muitas vezes em conjunto com Direct Connect Gateway para conexões físicas.

DIA DA PROVA

Estratégia de prova

A ANS-C01 é uma prova de cenários longos: uma empresa com muitas contas, VPCs, regiões e conexões híbridas, e um conjunto de requisitos que precisam ser atendidos ao mesmo tempo. As alternativas erradas costumam funcionar parcialmente, mas violam um requisito explícito (sem agentes, sem internet, menor esforço operacional, contas futuras, firewall de terceiros) ou não escalam. A banca prefere serviços gerenciados e nativos a scripts, instâncias EC2 e configuração conta a conta. Muitas vezes duas alternativas são tecnicamente possíveis e vence a que tem menor operação contínua ou a que respeita uma limitação do serviço, como não transitividade do peering ou ausência de propagação no peering de Transit Gateway.

Como responder

✓ Conheça o formato: 65 questões, das quais 50 contam para a nota e 15 não são pontuadas nem identificadas; trate todas como valendo.

✓ Responda todas: questão em branco conta como erro e não há penalidade por chute.

✓ Há múltipla escolha (uma certa em quatro) e múltipla resposta (duas ou mais certas em cinco ou mais); leia quantas o enunciado pede.

✓ Antes de ler as alternativas, sublinhe os qualificadores: menor esforço operacional, sem agentes, sem internet, contas atuais e futuras, menor custo, terceiros.

✓ Elimine primeiro os distratores clássicos: CloudTrail ou Config para medir desempenho, peering em malha para muitas VPCs, PrivateLink como roteador, scripts em EC2 ou Lambda quando há serviço gerenciado.

✓ Em perguntas de BGP, decida a direção do tráfego antes de escolher o atributo.

✓ Distribua a revisão pelos pesos: Network Design 30%, Network Implementation 26%, Network Security, Compliance, and Governance 24%, Network Management and Operation 20%.

✓ A nota é de 100 a 1.000, com mínimo de 750, e o modelo é compensatório: não é preciso passar em cada domínio, só no total.

Erros que derrubam candidatos

✗ Escolher ferramenta detectiva (Config, Security Hub) quando o enunciado pede impedir a ação.

✗ Usar CloudTrail, Config ou VPC Flow Logs para medir latência ou perda de pacotes.

✗ Esquecer que VPC peering não é transitivo e não aceita CIDRs sobrepostos.

✗ Inverter a direção do controle BGP entre local preference e communities ou AS path.

✗ Ignorar o appliance mode em inspeção stateful atrás do Transit Gateway.

✗ Superdimensionar: escolher Transit Gateway quando o cenário tem só duas VPCs e pede menor custo.

✗ Trocar CloudFront por Global Accelerator (e vice-versa) sem olhar protocolo e necessidade de IP estático.

Na semana da prova

- ☐ Refaça simulados completos e anote, para cada erro, qual requisito do enunciado a alternativa escolhida violou.
- ☐ Revise os quadros de comparação: as três ferramentas Monitor, os dois Analyzers, peering x Transit Gateway x Cloud WAN, CloudFront x Global Accelerator.
- ☐ Decore os números que caem: MTU 9001, 8500 e 1500; communities 7224:7300 e 7224:7100; 64:ff9b::/96.
- ☐ Desenhe de memória a inspeção central com Transit Gateway e o híbrido com Direct Connect gateway em duas localizações.
- ☐ Na véspera, revise só os itens de lembrar de cada capítulo e descanse.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Network Design

‣ dezenas de VPCs, várias contas, roteamento centralizado, adicionar VPCs sem novos peerings → **Transit Gateway compartilhado pelo RAM**

‣ segmentos globais definidos em política central, sem peering região a região → **AWS Cloud WAN**

‣ duas VPCs, sem planos de crescer, menor custo, muito tráfego → **VPC peering**

‣ on-premises não recebe rotas das VPCs novas atrás do Transit Gateway → **Allowed prefixes da associação DXGW-TGW**

‣ sobreviver à perda de uma localização Direct Connect inteira → **Conexões dedicadas em pelo menos duas localizações distintas**

⚠ O que o on-premises aprende é a lista de allowed prefixes da associação DXGW-TGW.

⚠ O DNS privado só vale na VPC do endpoint. Desative-o e associe private hosted zones às spokes.

⚠ Peering não é transitivo. Egress centralizado é via Transit Gateway.

2. Network Implementation

‣ o tráfego do data center às vezes sai pela VPN em vez do Direct Connect → **Local preference maior para rotas do DX no roteador on-premises**

‣ tráfego da AWS deve usar a conexão A e deixar a B como backup sem mudar prefixos → **Communities 7224:7300 na A e 7224:7100 na B**

‣ somar banda de vários túneis VPN enquanto o Direct Connect não fica pronto → **Várias VPNs com BGP e ECMP no Transit Gateway**

‣ VPN com desempenho ruim em longas distâncias → **VPN acelerada com Transit Gateway**

‣ túnel VPN cai quando fica sem tráfego → **Startup action Start e DPD timeout action Restart**

⚠ Rotas do TGW controlam a saída da AWS. A saída do data center se controla com local preference no roteador on-premises.

⚠ Prepending deixa a rota menos atrativa. Para a principal, community 7224:7300; para a backup, 7224:7100.

⚠ Prefixo mais específico atrai o tráfego para essa conexão, o oposto do desejado.

3. Network Management and Operation

‣ latência e perda até o on-premises, Direct Connect ou VPN, sem agentes → **CloudWatch Network Monitor**

‣ RTT e perda por fluxo entre instâncias ou VPCs, localizar o trecho degradado → **CloudWatch Network Flow Monitor**

‣ usuários na internet, desempenho por localização → **CloudWatch Internet Monitor**

‣ a rede da AWS entre AZs ou regiões teve latência maior, sem instalar nada → **Infrastructure Performance do Network Manager**

‣ por que A não alcança B, caminho salto a salto, sem agentes → **VPC Reachability Analyzer**

⚠ CloudTrail registra chamadas de API do plano de controle, não o plano de dados.

⚠ Config registra configuração e conformidade. Métricas e logs operacionais são CloudWatch.

⚠ Flow Logs não medem latência nem perda. Use Network Monitor, Network Flow Monitor ou Synthetics.

4. Network Security, Compliance, and Governance

‣ dezenas de contas, contas atuais e futuras, correção automática de WAF ou security groups → **AWS Firewall Manager com AWS Organizations**

‣ impedir em todas as contas, nenhuma conta pode, mesmo administradores → **SCP na OU correta**

‣ quem fez o quê, quando e de onde → **AWS CloudTrail (trail organizacional)**

‣ logs imutáveis, WORM, não podem ser apagados por administradores → **S3 Object Lock modo Compliance em conta de log archive**

‣ bloquear domínios maliciosos, exfiltração por DNS, sem agentes → **Route 53 Resolver DNS Firewall**

⚠ CloudTrail registra chamadas de API, não consultas DNS. Para DNS: Resolver query logging e DNS Firewall.

⚠ Config só detecta e corrige depois, com janela de exposição. Prevenção em todas as contas é SCP.

⚠ Negação na raiz atinge todas as contas, inclusive produção. Mova desenvolvimento para uma OU própria e anexe a SCP a ela.

GABARITO

Respostas do diagnóstico

D1. A) Usar um Transit Gateway centralizado com as VPCs atuais e futuras, com o tráfego entre elas controlado pelas tabelas de rotas dele → revise o capítulo 1

Por quê: Esta alternativa é a mais adequada porque a AWS Transit Gateway foi projetada exatamente para cenários de malha de múltiplas VPCs, contas e regiões, oferecendo um ponto central de conectividade. Ela permite anexar diversas VPCs, fazer compartilhamento via AWS RAM entre contas, e controlar o fluxo de tráfego com tabelas de rotas da própria Transit Gateway, reduzindo a complexidade operacional e facilitando a escalabilidade.

✗ B) Incorreta. Usar uma VPC de trânsito baseada em appliances EC2 introduz um ponto único de falha, aumenta a complexidade de operação (gerenciar instâncias, HA, updates) e limita a vazão em comparação com a Transit Gateway gerenciada pela...

✗ C) Incorreta. O VPC peering totalmente malhado não escala bem à medida que o número de VPCs cresce. É necessário criar e gerenciar manualmente muitos peerings e rotas, e não há um ponto central de controle de tráfego, dificultando a...

✗ D) Incorreta. AWS PrivateLink é ideal para expor serviços específicos (baseados em NLB) de forma privada, mas não é uma solução de roteamento de VPC-to-VPC full mesh.

> **Dica de prova:** Quando o requisito envolver muitas VPCs, múltiplas contas/regiões e necessidade de controle centralizado de tráfego (hub-and-spoke), pense primeiro em AWS Transit Gateway.

D2. B) Usar um Transit Gateway por região com peering entre eles, Direct Connect e VPN no de us-east-1 e rotas estáticas entre os Transit Gateways → revise o capítulo 1

Por quê: Esta alternativa usa AWS Transit Gateway em cada região, com peering entre TGWs, o que centraliza o roteamento regionalmente e reduz o número de túneis VPN. Ao conectar Direct Connect e VPN ao TGW principal (hub) e fazer peering inter-region, o tráfego híbrido pode ser distribuído de forma controlada para outras regiões. Além disso, o uso de tabelas de rotas do TGW e propagação/associação seletiva permite controlar quais VPCs em diferentes regiões podem se comunicar, evitando um full mesh obrigatório.

✗ A) Incorreta. Exige peering full mesh entre todas as VPCs em múltiplas regiões, o que não escala bem e não centraliza o controle de roteamento.

✗ C) Incorreta. Não existe 'VPC global' cobrindo múltiplas regiões; VPC é um constructo regional. Além disso, essa opção sugere um design não suportado e não utiliza os serviços gerenciados de roteamento (TGW), falhando em centralizar e escalar...

✗ D) Incorreta. AWS PrivateLink é indicado para exposição de serviços específicos (NLB/Interface Endpoint), não para roteamento geral entre VPCs.

> **Dica de prova:** Para cenários multi-região e híbridos, pense em AWS Transit Gateway como o 'core router' da AWS. Use TGW + inter-region peering para reduzir malha complexa de VPC peering e VPNs, e controle o alcance do tráfego com tabelas de rotas do TGW (associações e propagações seletivas).

D3. C) Usar um Transit Gateway em cada região com peering entre eles e várias tabelas de rotas para segmentar os domínios de produção e desenvolvimento → revise o capítulo 1

Por quê: A abordagem correta é usar AWS Transit Gateway em cada região, estabelecer peering entre Transit Gateways e configurar múltiplas tabelas de rotas no Transit Gateway para segmentar o tráfego. O AWS Transit Gateway atua como um hub que simplifica a conectividade entre múltiplas VPCs e redes on-premises, evitando a malha complexa de conexões ponto a ponto (full mesh).

✗ A) Incorreta. Concentra tudo em uma única VPC por região, o que não atende bem a cenários de múltiplas VPCs isoladas por domínio. Security Groups não substituem a necessidade de um mecanismo de roteamento centralizado e segmentado entre VPCs.

✗ B) Incorreta. VPC peering não escala bem para muitas VPCs, especialmente em múltiplas regiões, e não oferece tabelas de rotas centralizadas. Além disso, VPC peering é uma conexão ponto a ponto, sem o conceito de hub para governança central.

✗ D) Incorreta. Gera uma topologia de malha complexa e pouco escalável. A administração de múltiplos túneis VPN é difícil e não há o mesmo nível de centralização e segmentação que o Transit Gateway oferece.

D4. C) Ativar multicast no Transit Gateway, criar um multicast domain associado só às sub-redes envolvidas e registrar as ENIs como fontes e membros → revise o capítulo 2

Por quê: Esta alternativa é a correta porque o AWS Transit Gateway oferece suporte nativo a multicast por meio de domínios de multicast. Você pode habilitar multicast no Transit Gateway, criar um domínio de multicast e registrar as interfaces de rede (ENIs) das instâncias que precisam participar dos grupos.

✗ A) Incorreta. Um gateway de internet é voltado para tráfego entre VPC e internet pública, não para multicast interno. Além disso, rotas e security groups não transformam tráfego unicast em multicast, nem garantem o comportamento de replicação...

✗ B) Incorreta. Network Load Balancer não implementa multicast real. Ele distribui tráfego unicast para targets, não endereços de multicast.

✗ D) Incorreta. AWS PrivateLink é baseado em conexões unicast para serviços privados (endpoints de interface). Não há suporte a tráfego multicast ou a replicação de pacotes para múltiplos consumidores como em um grupo multicast.

> **Dica de prova:** Lembre que suporte a multicast em AWS é uma funcionalidade específica do AWS Transit Gateway. Se a questão mencionar multicast entre instâncias, grupos de multicast, domínios de multicast ou registro de ENIs, pense imediatamente em 'Transit Gateway multicast'.

D5. B) Usar uma conta central de DNS com endpoints do Route 53 Resolver e regras de encaminhamento compartilhadas pelo RAM e associadas às VPCs das várias regiões → revise o capítulo 2

Por quê: Esta alternativa é a mais adequada porque utiliza o modelo recomendado pela AWS para centralização de DNS entre múltiplas contas e VPCs: uma conta de DNS central com Amazon Route 53 Resolver, endpoints inbound/outbound e regras de encaminhamento compartilhadas via AWS RAM. Isso permite: - Administração centralizada de DNS, reduzindo esforço operacional e inconsistências. - Suporte multi-conta e multi-região, associando Resolver rules às VPCs em diferentes regiões.

✗ A) Incorreta. Exige gerenciamento de servidores EC2 (patching, HA, escalabilidade) e uso de peering de VPC em larga escala, o que não escala bem (limites de peering, gerenciamento complexo de rotas e transitive peering não suportado).

✗ C) Incorreta. AWS Managed Microsoft AD é voltado principalmente para identidade e integração com AD, não como solução principal de DNS multi-conta.

✗ D) Incorreta. Replicar zonas privadas em cada conta e região aumenta fortemente a complexidade operacional, risco de inconsistências e conflitos de nomes.

> **Dica de prova:** Em cenários de múltiplas contas e VPCs, pense em centralização + compartilhamento: conta de infraestrutura de rede, Route 53 Resolver (endpoints inbound/outbound) e AWS RAM para compartilhar regras entre contas. Servidores DNS baseados em EC2 geralmente são um último recurso, não a primeira escolha.

D6. D) Usar dois Transit Gateways (Prod e Não Prod), cada um com tabelas de rotas por função (serviços compartilhados, firewall, spokes) e associação e propagação seletivas → revise o capítulo 2

Por quê: Esta alternativa é a melhor solução porque combina segmentação lógica e controle de tráfego centralizado usando recursos nativos do AWS Transit Gateway. Ao separar TGWs por ambiente (Prod e Não Prod), você já obtém um nível forte de isolamento administrativo e de falha. Com o recurso de Route Table per Attachment e múltiplas tabelas de rotas do TGW, é possível: - Criar tabelas de rotas distintas para VPCs spoke, VPCs de serviços compartilhados e anexos de firewall/inspeção.

✗ A) Incorreta. Depende fortemente de rotas estáticas nas tabelas de rotas das VPCs, o que escala mal quando existem centenas de VPCs.

✗ B) Incorreta. Uma única tabela de rotas do TGW com propagação automática de todas as rotas cria uma topologia quase totalmente mesh.

✗ C) Incorreta. VPC peering em malha completa entre VPCs de Produção escala muito mal e complica o gerenciamento de rotas. Além disso, o peering não oferece um ponto central de aplicação de políticas de tráfego como o TGW.

> **Dica de prova:** - Para ambientes grandes, pense em AWS Transit Gateway como um roteador central com múltiplas VRFs lógicas (tabelas de rotas do TGW). Use associações e propagações seletivas para criar domínios de roteamento (por ambiente, por função, por zona de segurança).

D7. C) Usar um bucket S3 com Object Lock na conta de segurança, SCPs negando a exclusão de flow logs e buckets, e StackSets criando os flow logs em todas as contas → revise o capítulo 3

Por quê: Esta alternativa combina mecanismos de governança da organização (SCP), centralização de logs e imutabilidade com baixo esforço operacional contínuo. - A SCP não "obriga" diretamente a criação de Flow Logs, mas pode: - Negar a exclusão de Flow Logs e do bucket S3 central; - Restringir alterações de políticas que poderiam expor ou permitir a deleção dos logs.

✗ A) Incorreta. CloudTrail não substitui VPC Flow Logs; log de dados de VPC não cobre o mesmo nível de detalhe de tráfego IP/porta.

✗ B) Incorreta. VPC Flow Logs em Transit Gateway não substituem Flow Logs em cada VPC para visibilidade detalhada por interface ENI. Além disso, não atende ao requisito de habilitar Flow Logs em todas as VPCs;

✗ D) Incorreta. Usa AWS Config e Lambda, o que funciona, mas aumenta a complexidade operacional (funções Lambda, triggers, manutenção de código).

> **Dica de prova:** - Para requisitos de compliance e retenção longa de logs de rede, priorize S3 com versionamento + Object Lock (modo Compliance ou Governance) em uma conta de segurança dedicada.

D8. B) Usar VPC Flow Logs em um CloudWatch Logs central, com metric filters e alarmes que acionam o Systems Manager Automation ou o Lambda para respostas automáticas → revise o capítulo 3

Por quê: Esta alternativa é a melhor abordagem porque usa recursos nativos e gerenciados da AWS para monitoramento e automação em escala multi-conta. Ao habilitar VPC Flow Logs em todas as VPCs e direcioná-los para um grupo de logs central em Amazon CloudWatch Logs (via CloudWatch Logs Subscription Filters ou integração de contas), o time consegue uma visão consolidada do tráfego de rede sem precisar de agentes em cada instância.

✗ A) Incorreta. Depende de AWS Network Firewall em cada VPC, o que aumenta custos e complexidade de gestão. Além disso, o fluxo de trabalho descrito é essencialmente manual (consultas em Athena e scripts manuais), não atendendo bem ao requisito...

✗ C) Incorreta. Requer instalação e manutenção de agentes de terceiros em todas as instâncias EC2, o que aumenta o overhead operacional e a superfície de falha.

✗ D) Incorreta. AWS CloudTrail e AWS Config são excelentes para auditoria e conformidade de mudanças de configuração, mas não capturam detalhes de fluxo de tráfego de rede (camada de dados).

> **Dica de prova:** Para operações de rede em múltiplas contas, pense em três camadas: (1) Coleta centralizada de telemetria (VPC Flow Logs, DNS logs, etc.); (2) Normalização e criação de métricas (CloudWatch Metric Filters, métricas customizadas); (3) Automação de resposta (CloudWatch Alarms integrados com Lambda ou Systems Manager).

D9. A) Usar o Reachability Analyzer entre as ENIs de origem e destino, com análises entre contas habilitadas pela integração com o Organizations → revise o capítulo 3

Por quê: Esta alternativa é a melhor solução porque o AWS Reachability Analyzer faz análise de conectividade fim a fim em nível de plano de dados, construindo o caminho lógico que o tráfego percorreria entre dois recursos (como ENIs) e exibindo todos os saltos, incluindo VPCs, sub-redes, rotas, gateways e AWS Transit Gateway.

✗ B) Incorreta. VPC Flow Logs mostram aceitos/negados por ENI, mas não constroem automaticamente um caminho hop-by-hop detalhado, especialmente através de Transit Gateway.

✗ C) Incorreta. CloudTrail registra eventos de plano de controle (como alterações em rotas, anexos, etc.), não o fluxo de dados entre ENIs. Não é apropriado para rastrear o caminho efetivo que o tráfego segue na malha de rede.

✗ D) Incorreta. AWS Network Firewall é voltado para inspeção e filtragem de tráfego em nível de firewall. Usar seus logs apenas para descobrir o caminho completo seria excessivo, adicionaria custo e complexidade, e ainda assim não mostraria...

> **Dica de prova:** Para perguntas sobre visibilidade de caminho fim a fim na rede AWS (incluindo Transit Gateway e múltiplas VPCs) sem agentes, lembre-se do AWS Reachability Analyzer. Ele responde 'por onde o tráfego pode passar?' com base na configuração atual, enquanto VPC Flow Logs respondem 'o que passou e foi aceito/negado?'.

D10. A) MACsec na conexão dedicada, associando a chave CKN/CAK à conexão e configurando o roteador → revise o capítulo 4

Por quê: O MACsec (IEEE 802.1AE) criptografa o tráfego entre o roteador do cliente e o dispositivo da AWS no local do Direct Connect, com desempenho de taxa de linha. Está disponível em conexões dedicadas compatíveis (como 10 e 100 Gbps) e exige associar a chave CKN/CAK à conexão.

✗ B) Incorreta. VIFs não têm opção de criptografia TLS.

✗ C) Incorreta. Troca o Direct Connect pela internet e fica limitado à banda dos túneis.

✗ D) Incorreta. O Network Firewall inspeciona tráfego; não criptografa o enlace.

> **Dica de prova:** Criptografia de alta banda no Direct Connect dedicado: MACsec. Sem MACsec: VPN com IP privado sobre DX.

D11. A) AWS Firewall Manager → revise o capítulo 4

Por quê: O AWS Firewall Manager foi projetado para gerenciar, de forma centralizada, políticas de segurança de rede em ambientes multi-conta integrados ao AWS Organizations.

✗ B) Incorreta. O Control Tower governa a landing zone com controles, mas não gerencia o conteúdo dos security groups.

✗ C) Incorreta. O Security Hub consolida achados de conformidade; não aplica regras de security groups.

✗ D) Incorreta. O Config detecta e pode remediar configurações, mas não oferece políticas centrais de security groups entre contas como o Firewall Manager.

D12. A) Usar uma SCP negando a criação e a anexação de internet gateways, políticas de security groups do Firewall Manager e Network Firewall centralizado nas VPCs → revise o capítulo 4

Por quê: Esta alternativa é a melhor porque combina os mecanismos de governança adequados em cada camada: - SCP em AWS Organizations para negar 'ec2:CreateInternetGateway' e 'ec2:AttachInternetGateway' garante que nenhum Internet Gateway possa ser criado ou anexado em nenhuma conta, independentemente de permissões IAM locais, atendendo ao requisito (1) de forma preventiva e global.

✗ B) Incorreta. Políticas IAM em cada conta são mais frágeis e trabalhosas de manter do que SCPs em Organizations e podem ser modificadas por administradores da conta. Isso fere o requisito de governança forte para Internet Gateways.

✗ C) Incorreta. Negar apenas 'ec2:AuthorizeSecurityGroupIngress' é incompleto (não cobre egress nem outras ações em SGs). Além disso, AWS WAF em ALB não substitui AWS Network Firewall como camada de inspeção centralizada de tráfego de rede em...

✗ D) Incorreta. NACLs não impedem a criação ou anexação de Internet Gateways, apenas controlam tráfego em nível de subnet. Depender apenas de AWS Config + remediação é reativo e não impede a criação de recursos indevidos;

> **Dica de prova:** - Para bloquear criação/uso de recursos em TODAS as contas, pense primeiro em Service Control Policies (SCPs) em AWS Organizations, e não em IAM local. - Para políticas de segurança de rede consistentes em múltiplas contas/VPCs (Security Groups, Network Firewall, WAF), lembre-se do AWS Firewall Manager como a...

Agora, treine no formato real

Faça as 6 provas completas do curso ANS-C01: 390 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de Amazon Web Services (AWS). As questões são inéditas e não reproduzem a prova real.