AWS Academy Cloud Foundations (Fundamentos de nuvem da AWS Academy)

Módulo 9: Arquitetura de nuvem

aws academy

Visão geral do módulo

Tópicos

- AWS Well-Architected Framework
- Confiabilidade e alta disponibilidade
- AWS Trusted Advisor

Atividades

- Princípios de design do AWS Well-Architected Framework
- Interpretar as recomendações do AWS Trusted Advisor

Teste de conhecimento

Objetivos do módulo

Depois de concluir este módulo, você deverá ser capaz de:

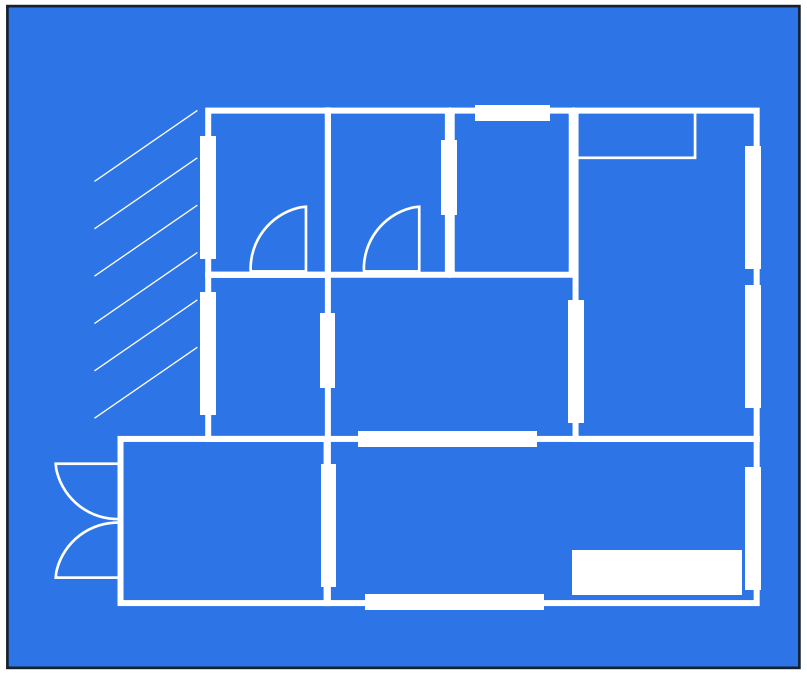
- Descrever o AWS Well-Architected Framework, incluindo os cinco pilares
- Identificar os princípios de design do AWS Well-Architected Framework
- Explicar a importância da confiabilidade e da alta disponibilidade
- Identificar como o AWS Trusted Advisor ajuda os clientes
- Interpretar as recomendações do AWS Trusted Advisor

Módulo 9: Arquitetura de nuvem

Seção 1: AWS Well-Architected Framework

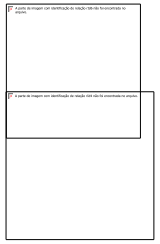
aws academy

Arquitetura: projeto e criação

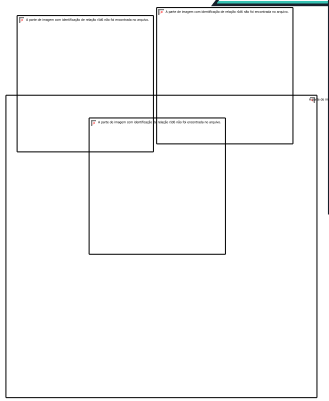


Design de estrutura

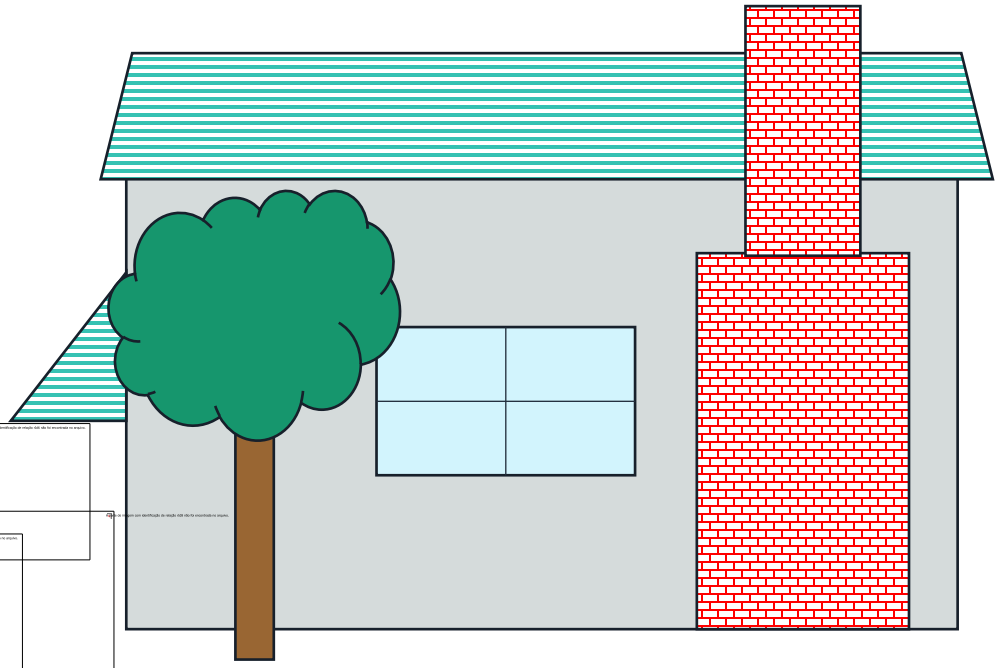
Cliente
(Tomador de decisão)



Architect



Equipe de criação
(Equipe de entrega)

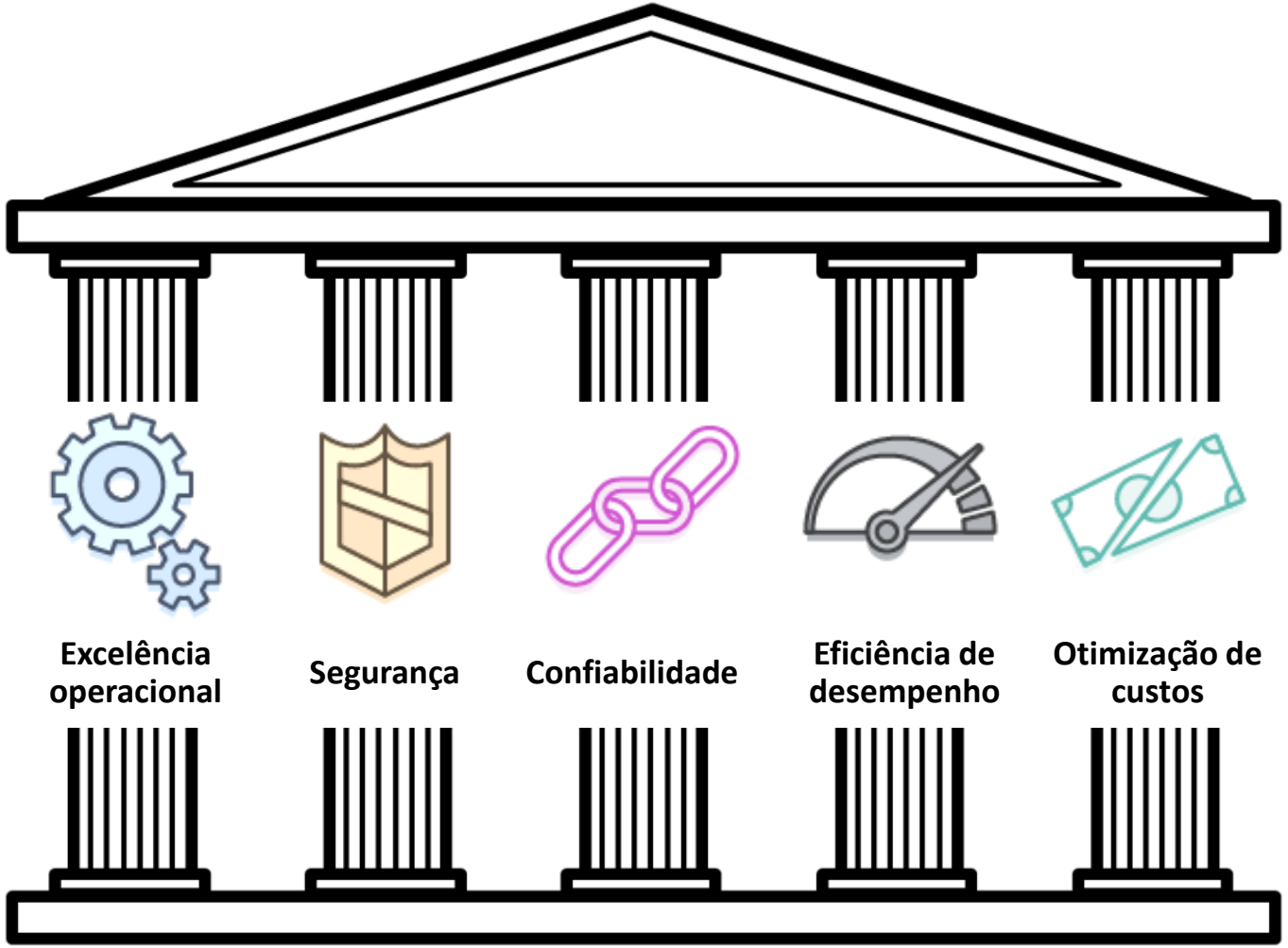


Estrutura concluída

O que é o AWS Well-Architected Framework?

- Um guia para projetar infraestruturas que são:
  - ✓Seguro
  - ✓Alta performance
  - ✓Resiliente
  - ✓Eficientes
- Uma abordagem consistente para avaliar e implementar arquiteturas de nuvem
- Uma maneira de fornecer melhores práticas que foram desenvolvidas a partir das lições aprendidas durante análises de arquiteturas de clientes

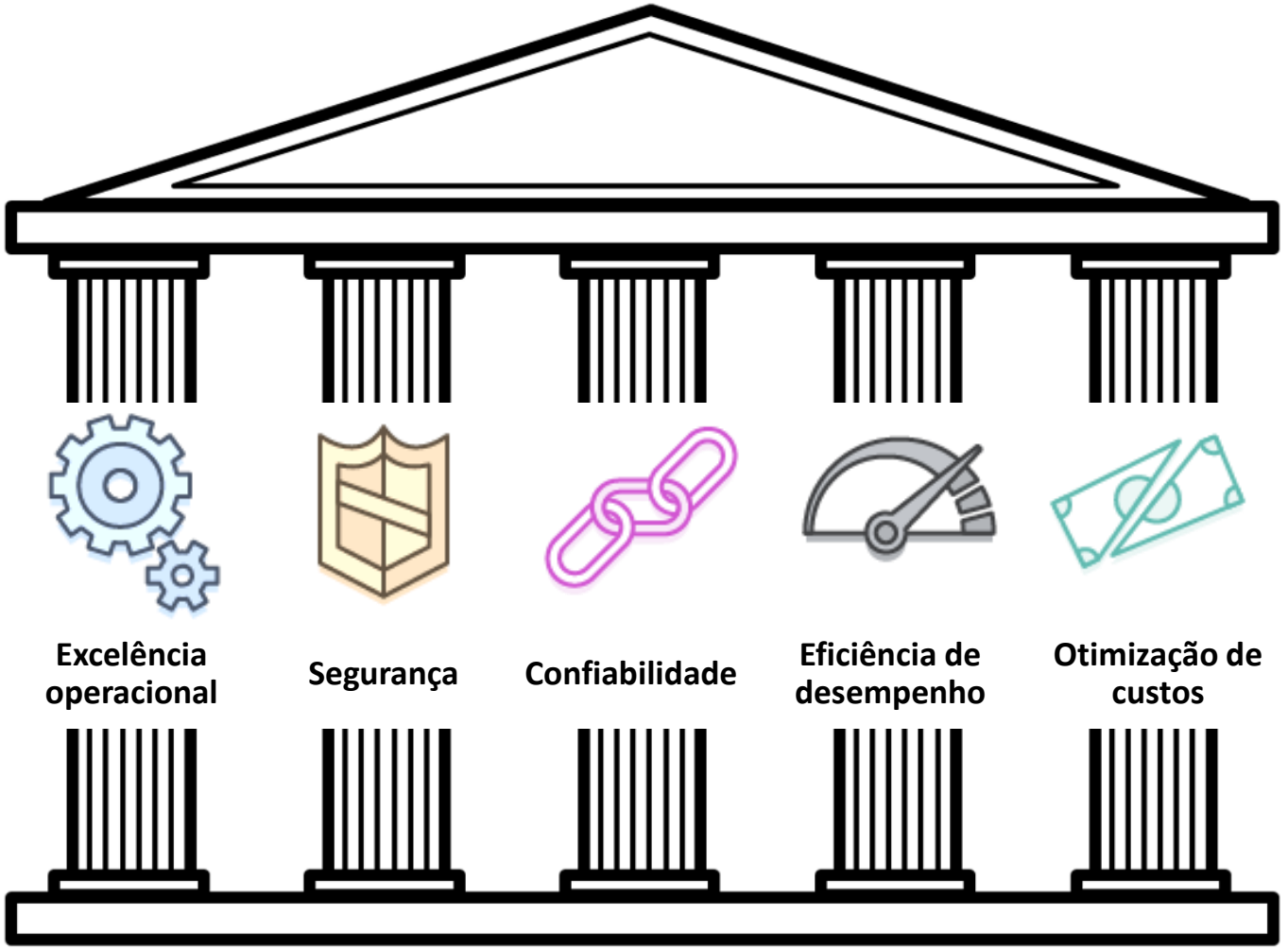
Pilares do AWS Well-Architected Framework



Organização do pilar

Área de melhores práticas	**Identity and Access Management**
Texto da pergunta	**SEG 1: Como gerenciar credenciais e autenticação?**
Contexto da pergunta	Os mecanismos de credenciais e autenticação incluem senhas, tokens e chaves que concedem acesso direto ou indireto à sua carga de trabalho. Proteja credenciais com mecanismos apropriados para ajudar a reduzir o risco de uso acidental ou mal-intencionado.
Melhores práticas	Melhores práticas: • Definir requisitos para o gerenciamento de identidade e acesso • Proteger o usuário raiz da conta da AWS • Aplicar o uso da autenticação multifator • Automatizar a aplicação de controles de acesso • Integrar-se ao provedor de federação centralizado • Aplicar requisitos de senha • Alternar as credenciais regularmente • Fazer auditoria periódica das credenciais

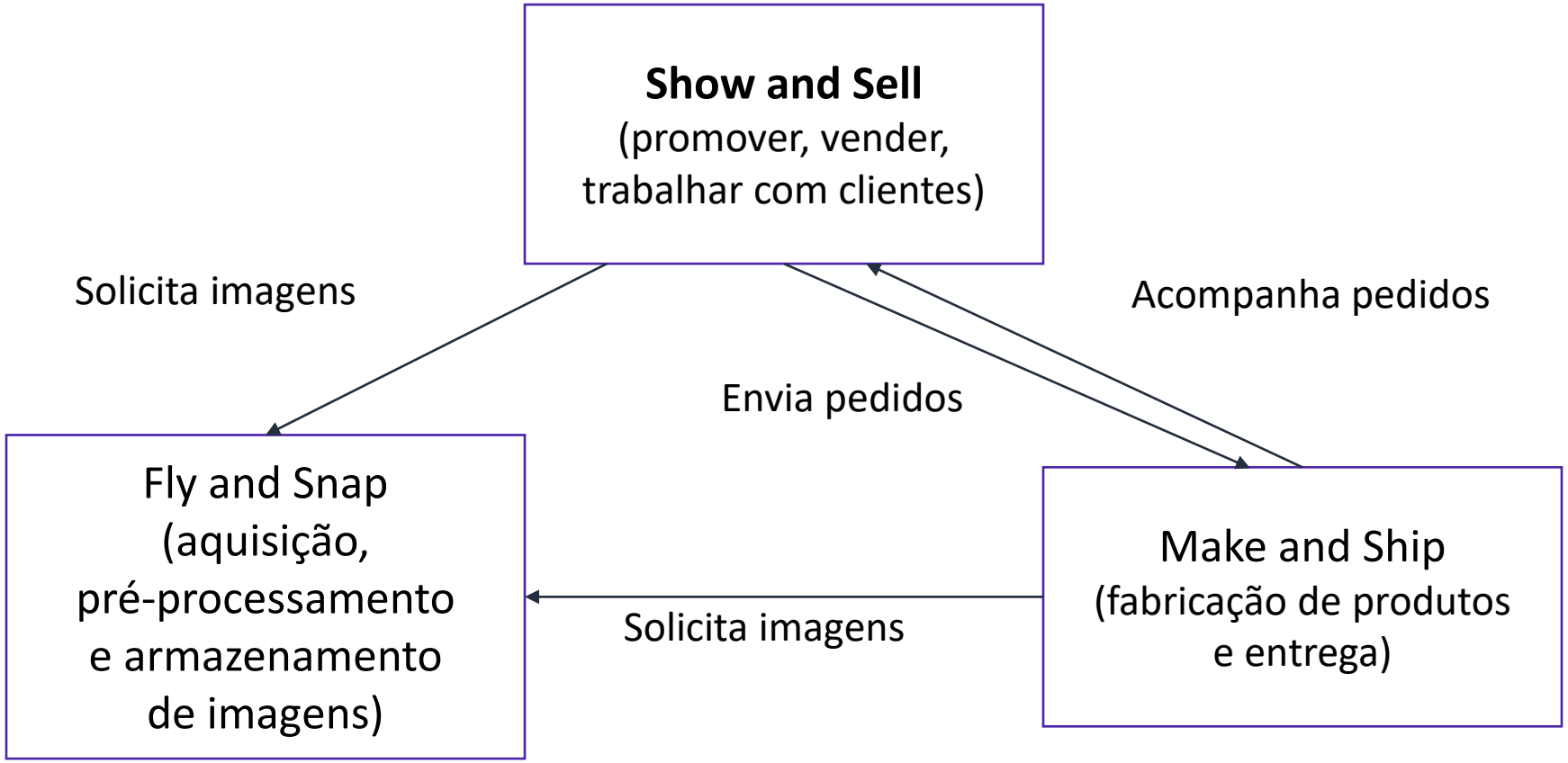
Introdução à atividade dos princípios de design do AWS Well-Architected Framework



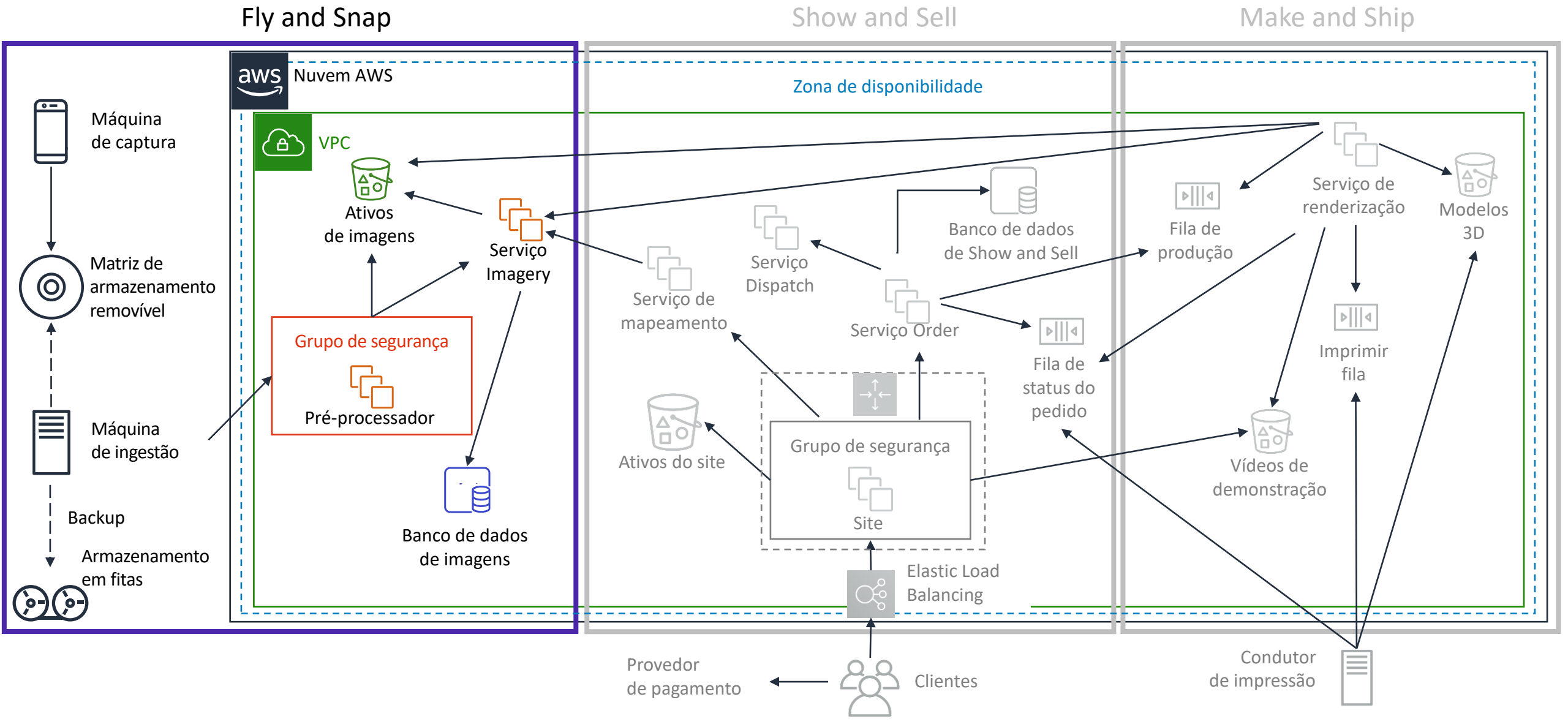
Histórico da AnyCompany

- AnyCompany Corporation: "*Paisagens urbanas em que você pode entrar*"
- Fundada em 2008 por John Doe
- Vende imagens 3D impressas de paisagens urbanas
- Prestes a se inscrever para investimento
- Solicitou que **você** realizasse uma análise de sua plataforma como parte da auditoria
- Nativo da nuvem

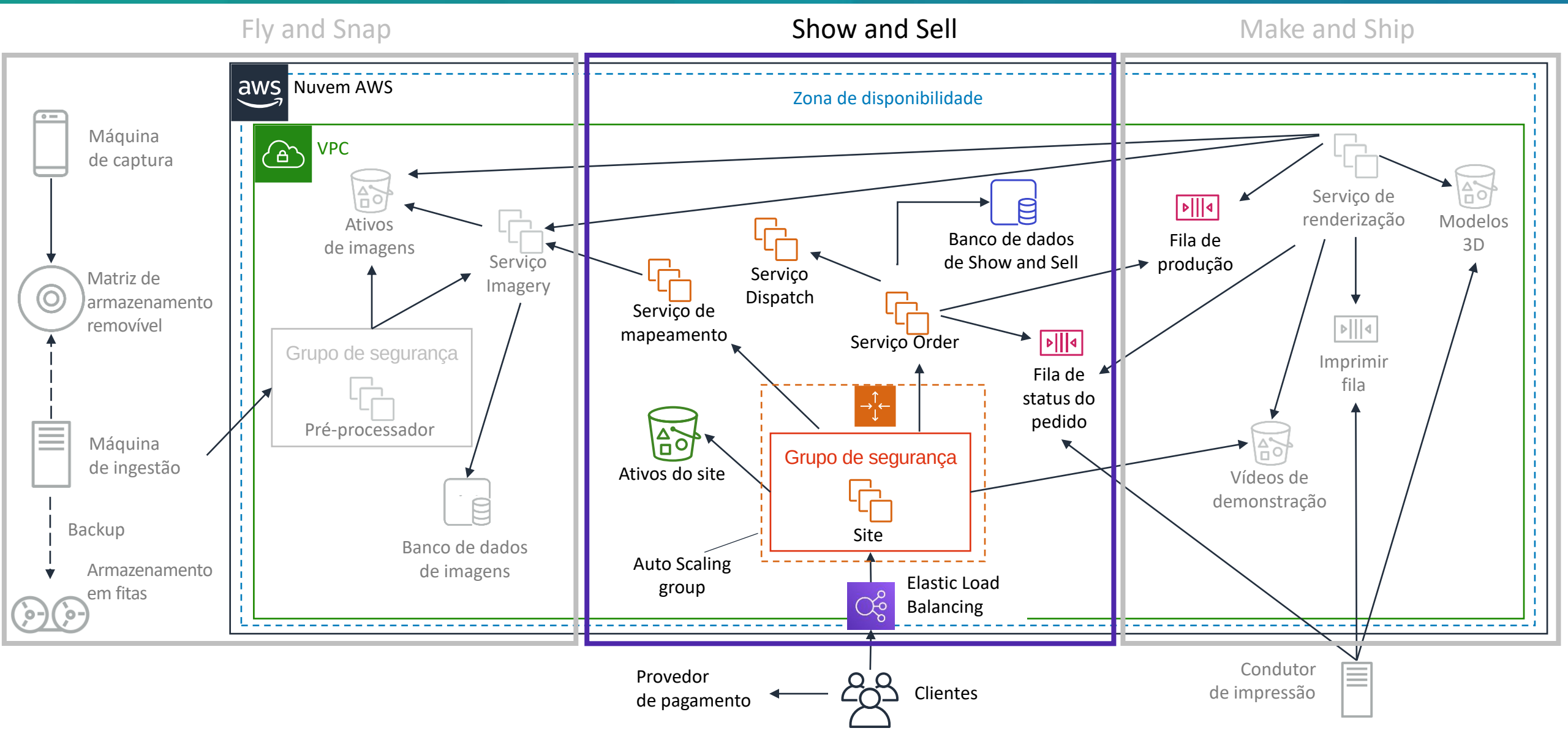
Histórico da AnyCompany (continuação)



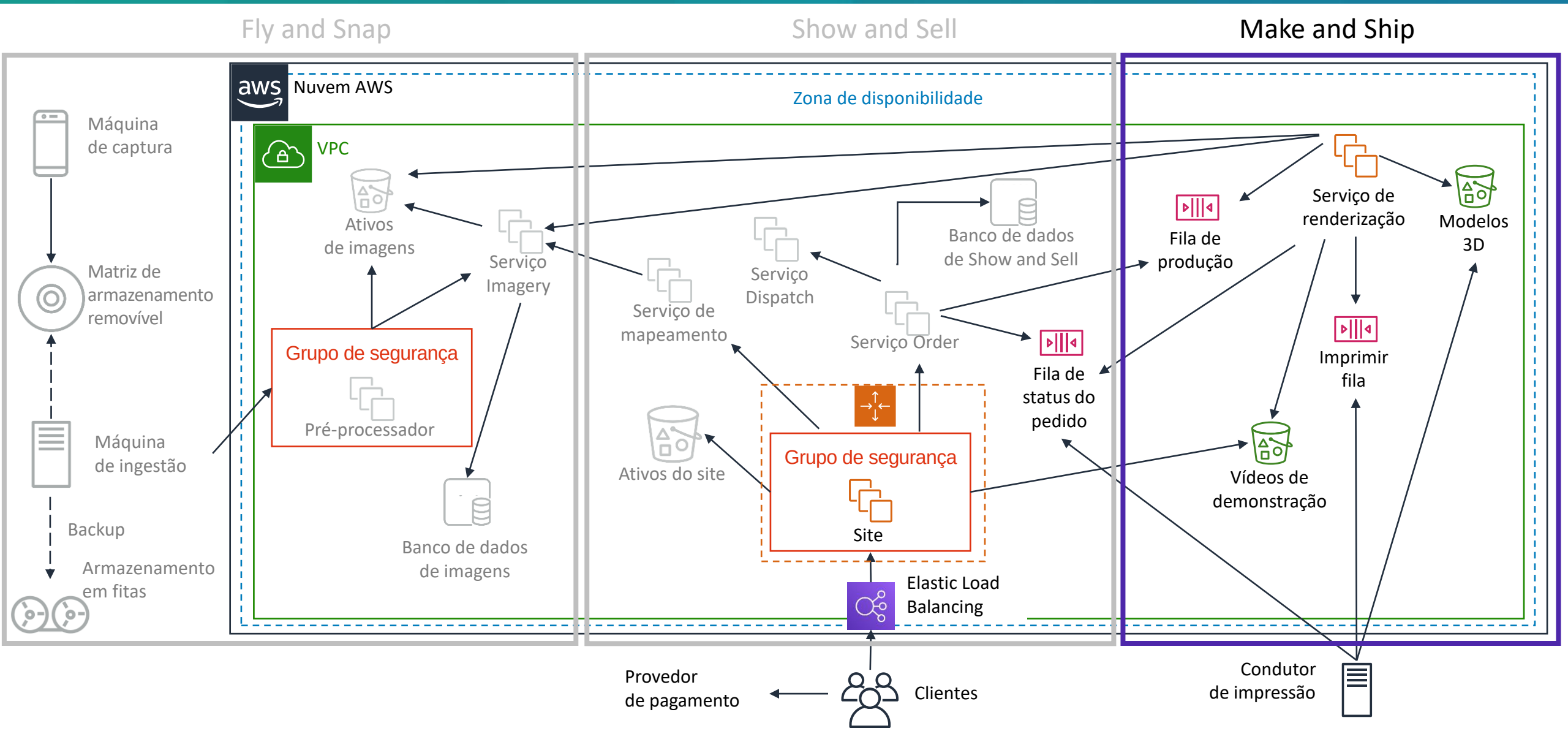
Arquitetura da AnyCompany: Fly and Snap



Arquitetura da AnyCompany: Show and Sell



Arquitetura da AnyCompany: Make and Ship



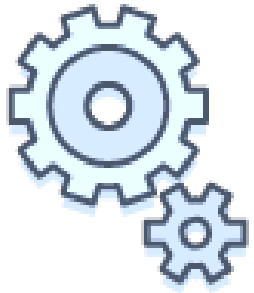
Visão geral da atividade

- Divida em pequenos grupos.
- Você aprenderá sobre cada um dos pilares. No final de cada pilar, há um conjunto de perguntas do AWS Well-Architected Framework para você responder com seu grupo. Use essas perguntas do Framework para orientar sua análise da arquitetura da AnyCompany.
- Para cada pergunta sobre o Well-Architected Framework, responda às seguintes perguntas sobre a arquitetura da AnyCompany:
  - Qual é o ESTADO ATUAL (o que a AnyCompany está fazendo no momento)?
  - Qual é o ESTADO FUTURO (o que você acha que a AnyCompany deveria estar fazendo?)
- Concorde com a melhoria mais importante para a AnyCompany realizar em sua arquitetura para cada conjunto de perguntas do Well-Architected Framework.
- Dica: não há respostas certas ou erradas.

Pilar Excelência operacional

Pilar Excelência operacional

Pilar Excelência operacional

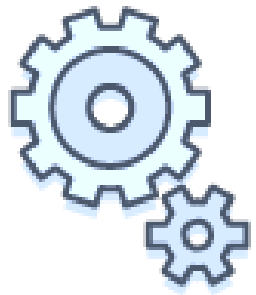


Entregar valor comerciial

- Foco
  - Executar e monitorar sistemas para agregar valor comercial e melhorar continuamente os processos e procedimentos de suporte.
- Principais tópicos
  - Gerenciar e automatizar alterações
  - Responder a eventos
  - Definir padrões para gerenciar com êxito as operações diárias

Princípios de design de excelência operacional

Pilar Excelência operacional



Entregar valor comerciial

- Executar operações como código
- Anotar a documentação
- Fazer alterações frequentes, pequenas e reversíveis
- Refinar os procedimentos operacionais com frequência
- Prever falhas
- Aprender com eventos e falhas operacionais

Perguntas sobre excelência operacional

Preparação

- Como determinar quais são suas prioridades?
- Como você projeta a carga de trabalho para que possa compreender seu estado?
- Como você reduz defeitos, facilita a correção e melhora o fluxo para a produção?
- Como você mitiga os riscos de implantação?
- Como você sabe se está pronto para oferecer suporte a uma carga de trabalho?

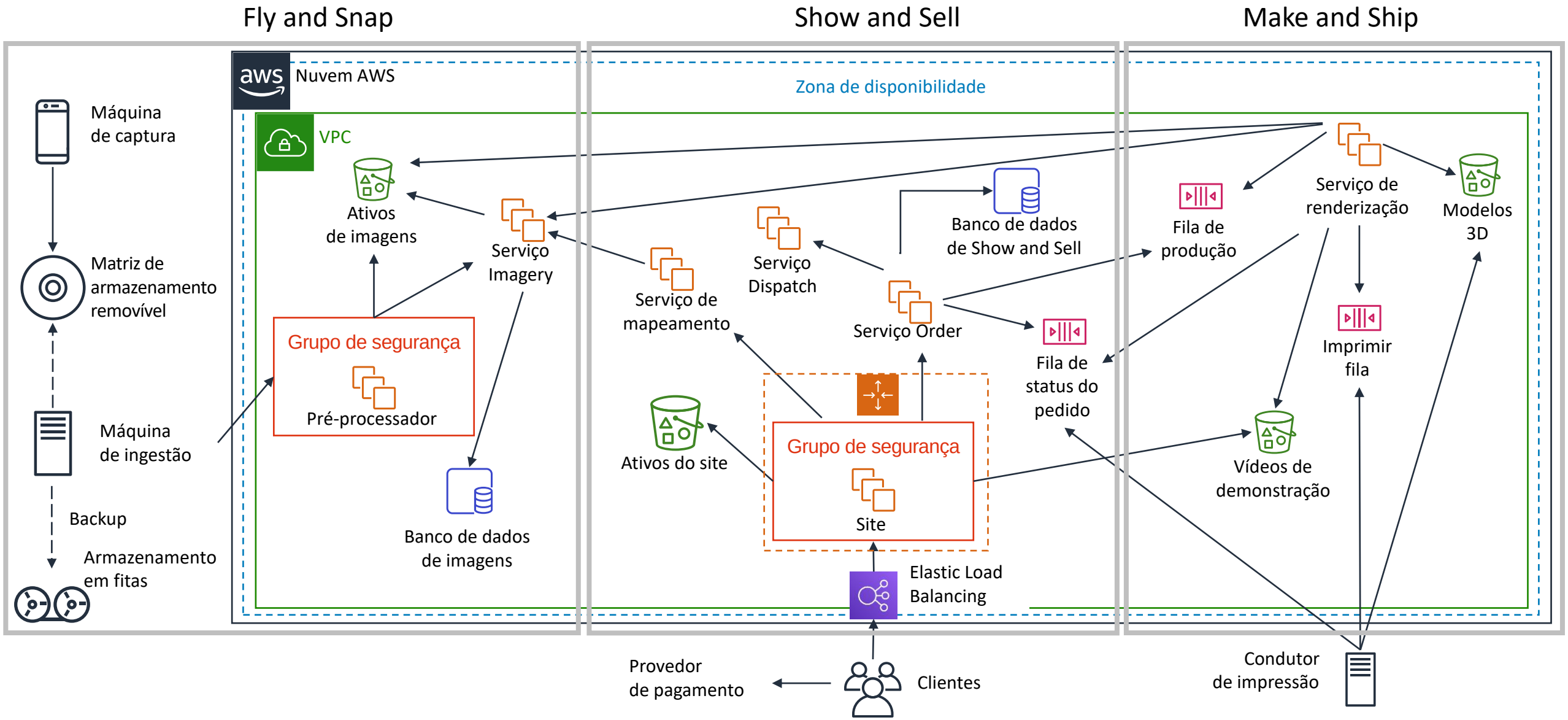
Execução

- Como você compreende a integridade de sua carga de trabalho?
- Como você compreende a integridade de suas operações?
- Como você gerencia eventos de carga de trabalho e de operações?

Evolução

- Como você evolui as operações?

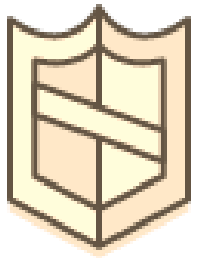
Detalhamento de atividade



Pilar Segurança

Pilar Segurança

Segurança pilar

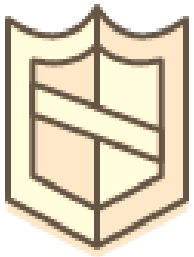


Proteger e monitorar sistemas

- Foco
  - Proteger informações, sistemas e ativos, e ao mesmo tempo agregar valor comercial por meio de avaliações de risco e estratégias de mitigação.
- Principais tópicos
  - Identificar e gerenciar quem pode fazer o quê
  - Estabelecimento de controles para detectar eventos de segurança
  - Proteção de sistemas e serviços
  - Confidencialidade e integridade dos dados

Princípios de design de segurança

Segurança pilar



Proteger e monitorar sistemas

- Implementar uma base de identidade sólida
- Habilitar a rastreabilidade
- Aplicar segurança em todas as camadas
- Automatizar as melhores práticas de segurança
- Proteger dados em trânsito e ociosos
- Manter as pessoas longe dos dados
- Preparar-se para eventos de segurança.

Perguntas sobre segurança

Identity and access management

- Como você gerencia credenciais e autenticação?
- Como você controla o acesso humano?
- Como você controla o acesso programático?

Controles de detecção

- Como você detecta e investiga eventos de segurança?
- Como você se defende de ameaças à segurança emergentes?

Proteção de infraestrutura

- Como você protege as redes?
- Como você protege os recursos de computação?

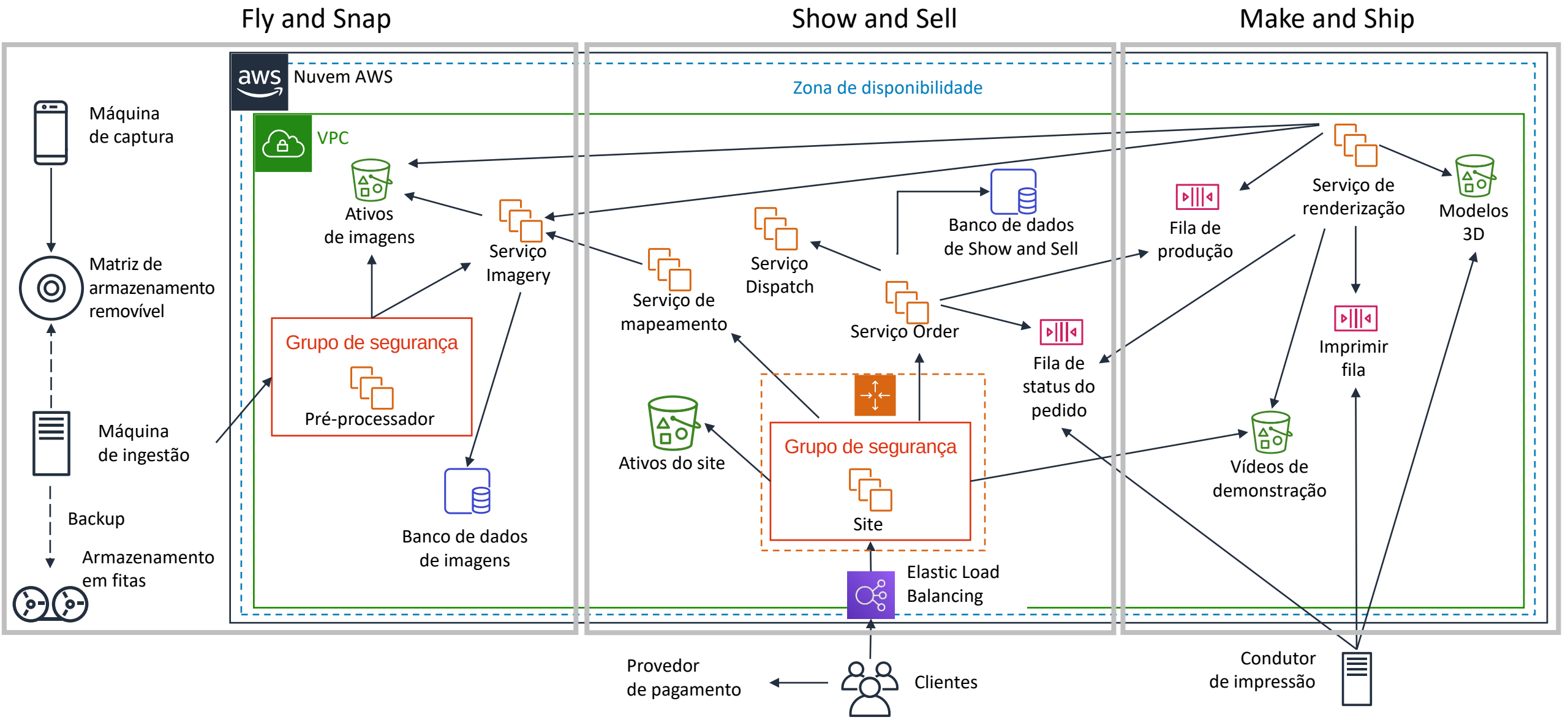
Proteção de dados

- Como você classifica os dados?
- Como você protege os dados ociosos?
- Como você protege os dados em trânsito?

Resposta a incidentes

- Como você responde a um incidente?

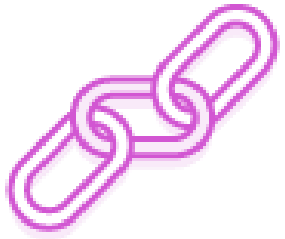
Detalhamento de atividade



Pilar Confiabilidade

Pilar Confiabilidade

Pilar Confiabilidade

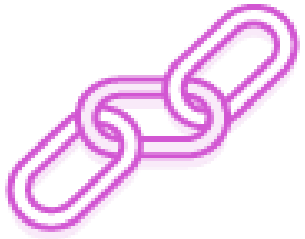


Recupere-se de falhas e reduza interrupções.

- Foco
  - Previna-se e recupere-se rapidamente de falhas para atender à demanda dos negócios e dos clientes.
- Principais tópicos
  - Configuração
  - Requisitos entre projetos
  - Planejamento de recuperação
  - Tratamento de alterações

Princípios de design de confiabilidade

Pilar Confiabilidade



Recupere-se de falhas e reduza interrupções.

- Testar procedimentos de recuperação
- Recuperar-se automaticamente de falhas
- Escale horizontalmente para aumentar a disponibilidade agregada do sistema.
- Pare de tentar adivinhar a capacidade
- Gerenciar alterações na automação

Perguntas sobre confiabilidade

Fundamentos

- Como você gerencia service limits?
- Como você gerencia a topologia de rede?

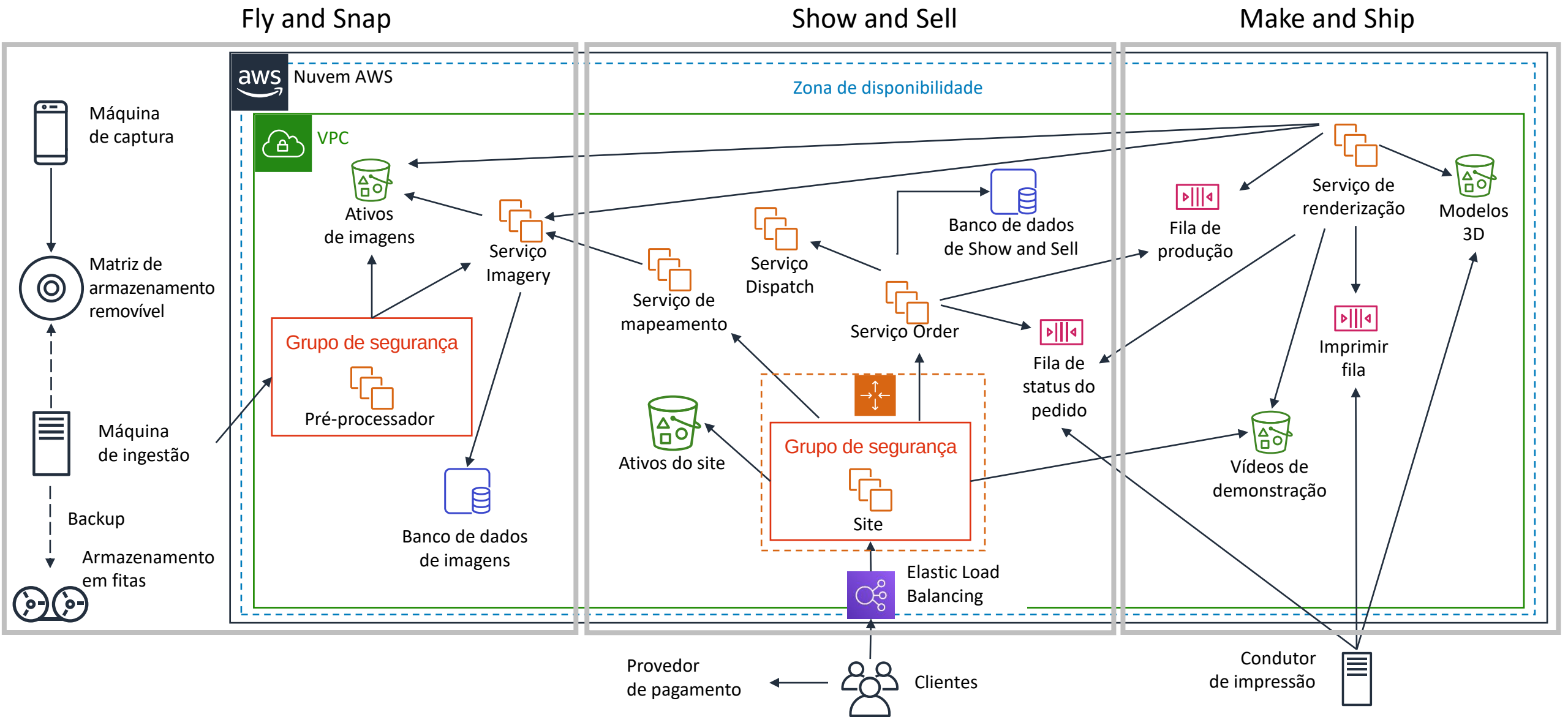
Gerenciamento de alterações

- Como o sistema se adapta às alterações na demanda?
- Como você monitora os recursos?
- Como você implementa alterações?

Gerenciamento de falhas

- Como você faz backup de dados?
- Como o seu sistema lida com falhas de componentes?
- Como você testa a resiliência?
- Como você planeja a recuperação de desastres?

Detalhamento de atividade



Pilar Eficiência de desempenho

Pilar Eficiência de desempenho

Eficiência de desempenho pilar

Use os recursos com moderação.

- Foco
  - Use os recursos de computação e TI de forma eficiente para atender aos requisitos do sistema e manter essa eficiência à medida que as mudanças na demanda e as tecnologias evoluem.
- Principais tópicos
  - Seleção dos tipos e tamanhos certos de recursos com base nos requisitos de carga de trabalho
  - Monitoramento e desempenho
  - Tomar decisões embasadas para manter a eficiência à medida que as necessidades empresariais evoluem

Princípios de projeto da eficiência de desempenho

Eficiência de desempenho pilar

Use os recursos com moderação.

- Democratizar tecnologias avançadas
- Tenha alcance global em minutos
- Usar arquiteturas sem servidor
- Experimentar com mais frequência
- Ter afinidade mecânica

Perguntas sobre eficiência de desempenho

Seleção

- Como você seleciona a arquitetura que tem melhor desempenho?
- Como você seleciona sua solução de computação?
- Como você seleciona sua solução de armazenamento?
- Como você seleciona sua solução de banco de dados?
- Como você seleciona sua solução de rede?

Revisão

- Como você evolui sua carga de trabalho para aproveitar as novas versões?

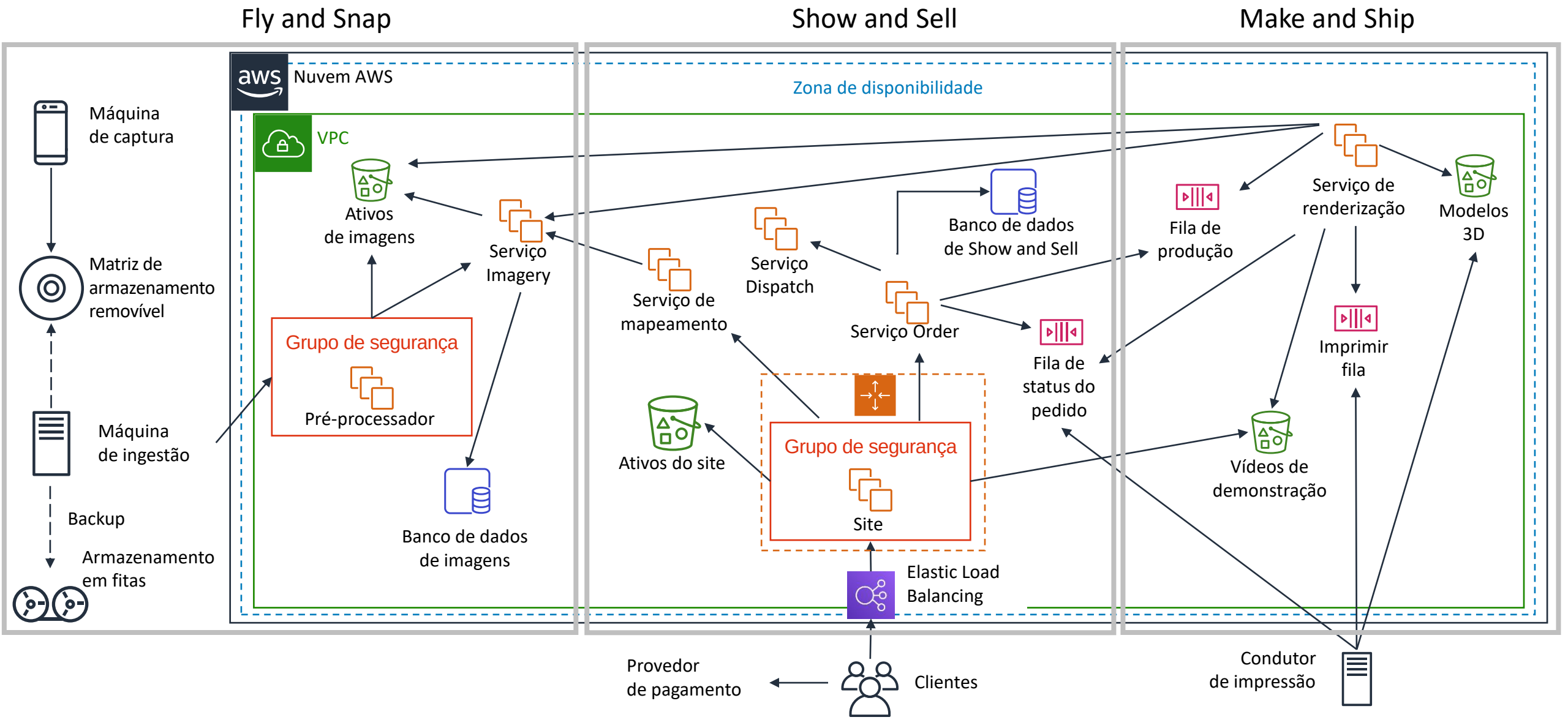
Monitoramento

- Como você monitora seus recursos para garantir que eles estejam funcionando conforme o esperado?

Vantagens e desvantagens

- Como usar compensações para melhorar o desempenho?

Detalhamento de atividade



Pilar Otimização de custos

Pilar Otimização de custos

Pilar Otimização de custos

Elimine despesas desnecessárias.

- Foco
  - Execute sistemas para agregar valor comercial pelo menor preço.
- Principais tópicos
  - Compreender e controlar quando o dinheiro está sendo gasto
  - Selecionar o número mais apropriado e correto de tipos de recursos
  - Analisar gastos ao longo do tempo
  - Escalabilidade para atender às necessidades empresariais sem gastos excessivos

Princípios de design de otimização de custos

Pilar Otimização de custos

Elimine despesas desnecessárias.

- Adotar um modelo de consumo
- Medir a eficiência geral
- Eliminar despesas em operações de datacenter
- Analisar e atribuir despesas
- Usar serviços gerenciados e em nível de aplicativo para reduzir o custo de propriedade

Perguntas sobre otimização de custos

Visibilidade de gastos

- Como você controla o uso?
- Como você monitora o uso e o custo?
- Como você descomissiona recursos?

Recursos de baixo custo

- Como você avalia o custo ao selecionar serviços?
- Como você cumpre metas de custo ao selecionar o tipo e o tamanho do recurso?
- Como usa modelos de definição de preço para reduzir custos?
- Como você planeja alterações de transferência de dados?

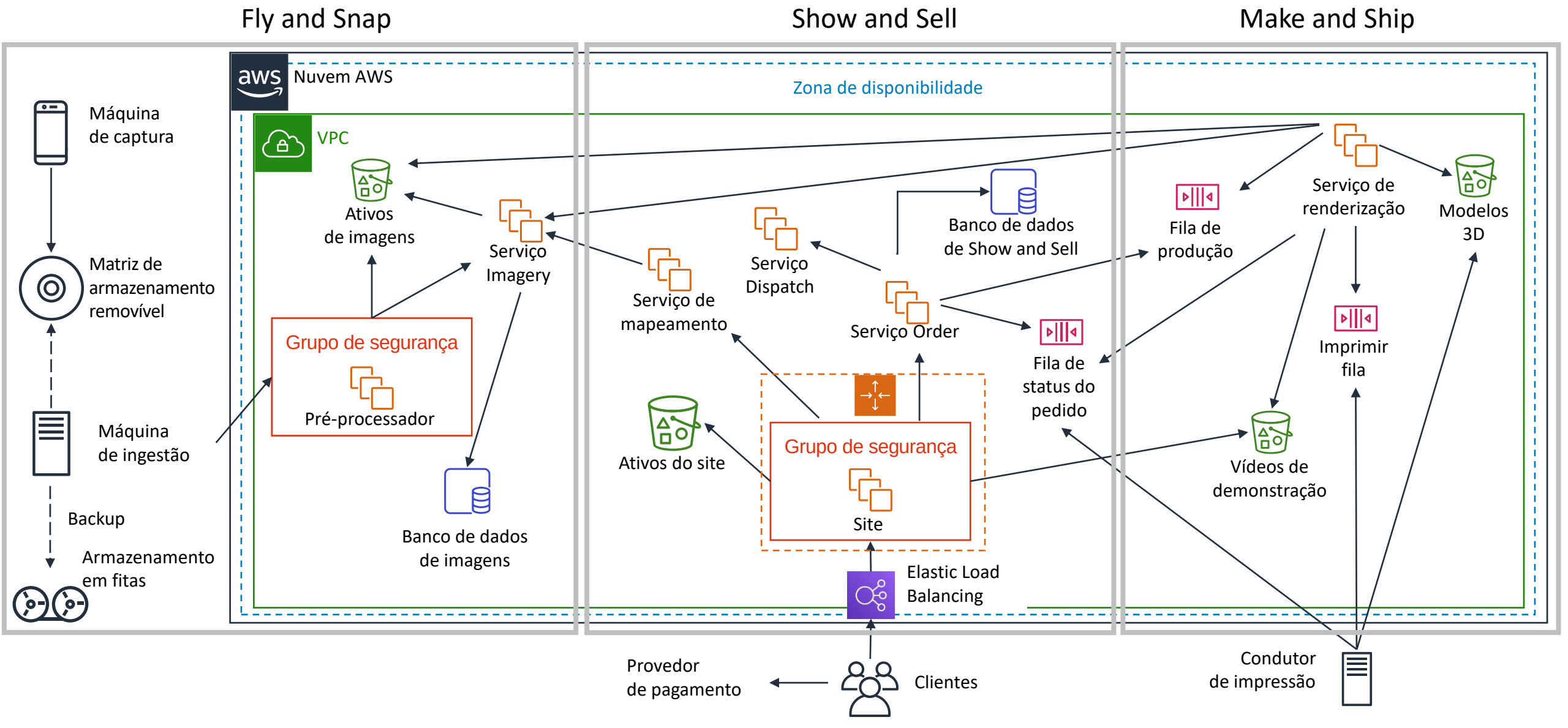
Correspondência de oferta e demanda

- Como você faz a correspondência entre a oferta de recursos e a demanda?

Otimização ao longo do tempo

- Como você avalia novos serviços?

Detalhamento de atividade



AWS Well-Architected Tool

- Ajuda a analisar o estado das cargas de trabalho e as compara com as mais recentes melhores práticas de arquitetura da AWS.
- Oferece acesso ao conhecimento e às melhores práticas usados pelos arquitetos da AWS sempre que necessário
- Fornece um plano de ação com orientações passo a passo de como criar melhores cargas de trabalho para a nuvem
- Oferece um processo consistente para você analisar e medir suas arquiteturas de nuvem

Principais lições da Seção 1

- O AWS Well-Architected Framework fornece uma abordagem consistente para avaliar arquiteturas de nuvem e orientações para ajudar a implementar projetos.
- O AWS Well-Architected Framework documenta um conjunto de perguntas básicas que permitem entender como uma arquitetura específica se alinha às melhores práticas da nuvem.
- O AWS Well-Architected Framework está organizado em cinco pilares.
- Cada pilar inclui um conjunto de princípios de design e melhores práticas.

Módulo 9: Arquitetura de nuvem

Seção 2: Confiabilidade e disponibilidade

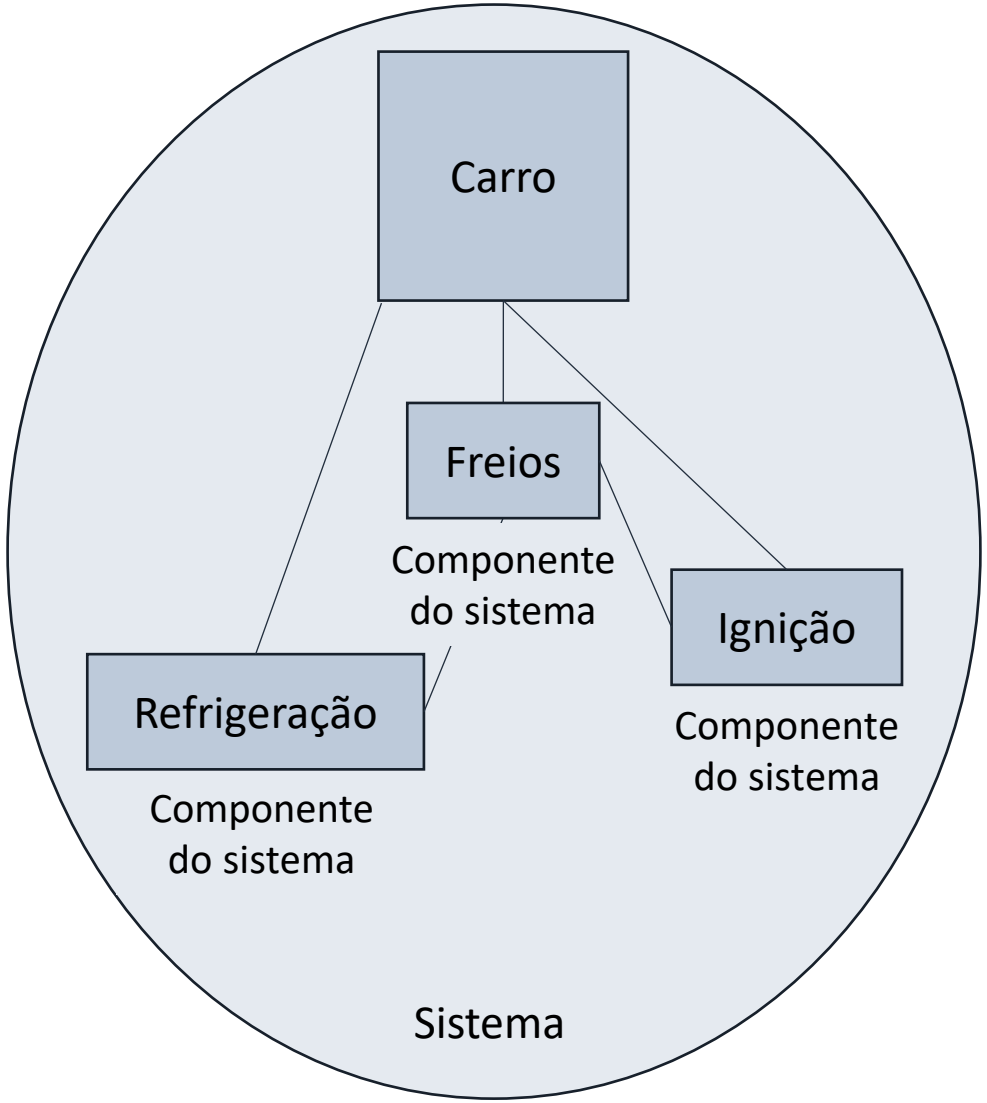
aws academy

“Tudo falha, o tempo todo”.

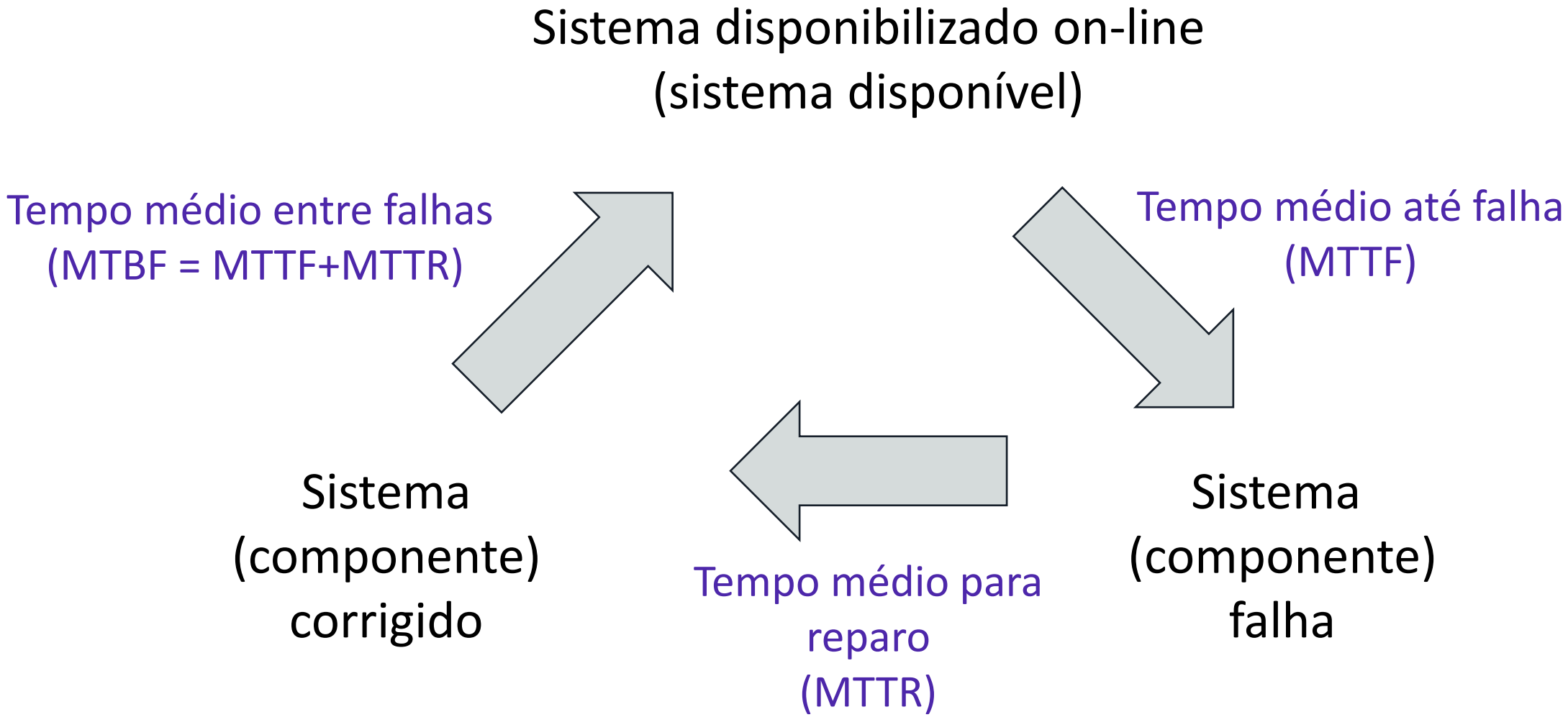
Werner Vogels, diretor de tecnologia da Amazon.com

Confiabilidade

- Uma medida da capacidade do sistema de fornecer funcionalidade quando o usuário quiser.
- O sistema inclui todos os componentes do sistema: hardware, firmware e software.
- Probabilidade de que todo o sistema funcione como pretendido por um período especificado.
- Tempo médio entre falhas (MTBF) = tempo total em serviço/número de falhas



Noções básicas sobre métricas de confiabilidade



Disponibilidade

- Tempo normal de operação/tempo total
- Uma porcentagem do tempo de atividade (por exemplo, 99,9%) ao longo do tempo (por exemplo, 1 ano)
- Número de noves - Cinco noves significam disponibilidade de 99,999%

Alta disponibilidade

- O sistema pode suportar alguma medida de degradação e ainda permanecer disponível.
- O tempo de inatividade é minimizado
- Necessidade mínima de intervenção humana

Níveis de disponibilidade

Availability	Max Disruption (per year)	Application Category
99%	3 days 15 hours	Batch processing, data extraction, transfer, and load jobs
99.9%	8 hours 45 minutes	Internal tools like knowledge management, project tracking
99.95%	4 hours 22 minutes	Online commerce, point of sale
99.99%	52 minutes	Video delivery, broadcast systems
99.999%	5 minutes	ATM transactions, telecommunications systems

Fatores que influenciam a disponibilidade

Tolerância a falhas

- A redundância integrada dos componentes de um aplicativo e sua capacidade de permanecer operacional.

Escalabilidade

- A capacidade de um aplicativo acomodar aumentos nas necessidades de capacidade sem alterar o design.

Capacidade de recuperação

- O processo, as políticas e os procedimentos relacionados ao serviço de restauração após um evento catastrófico.

Principais lições da Seção 2

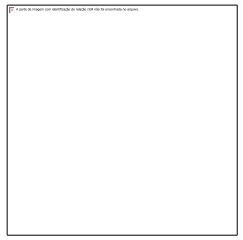
- Confiabilidade é uma medida da capacidade do sistema de fornecer funcionalidade quando o usuário quiser, e isso pode ser medido em termos de MTBF.
- Disponibilidade é a porcentagem de tempo em que um sistema opera normalmente ou executa corretamente as operações esperadas dele (ou o tempo normal de operação ao longo do tempo total).
- Três fatores que influenciam a disponibilidade dos aplicativos são tolerância a falhas, escalabilidade e capacidade de recuperação.
- Você pode projetar cargas de trabalho e aplicativos para serem altamente disponíveis, mas há uma compensação de custo a considerar.

Módulo 9: Arquitetura de nuvem

Seção 3: AWS Trusted Advisor

aws academy

AWS Trusted Advisor



AWS Trusted Advisor

- Ferramenta on-line que fornece orientações em tempo real para ajudar você a provisionar seus recursos de acordo com as melhores práticas da AWS.
- Examina todo o seu ambiente da AWS e oferece recomendações em tempo real em cinco categorias.

Otimização de custos

0 ✓ 9 ⚠ 0 !

$7,516.85

Possíveis economias mensais

Desempenho

3 ✓ 7 ⚠ 0 !

Segurança

2 ✓ 4 ⚠ 11 !

Tolerância a falhas

0 ✓ 15 ⚠ 5 !

Service Limits

37 ✓ 0 ⚠ 1 !

Atividade: Interpretar as recomendações do AWS Trusted Advisor

aws academy

Otimização de custos

0 ✓ 9 ⚠ 0 !

7.516,85 USD

Possíveis economias mensais

Desempenho

3 ✓ 7 ⚠ 0 !

Segurança

2 ✓ 4 ⚠ 11 !

Tolerância a falhas

0 ✓ 15 ⚠ 5 !

Service Limits

37 ✓ 0 ⚠ 1 !

Atividade: Recomendação nº 1

MFA na conta raiz

Descrição: Verifica a conta raiz e alerta se a autenticação MFA (multi-factor authentication) não está habilitada. Para ter mais segurança, recomendamos que você proteja a sua conta usando a MFA, que requer que o usuário insira um código único de autenticação do seu dispositivo físico ou virtual de MFA ao interagir com o Console AWS e sites associados.

Critérios de alerta: a MFA não está habilitada na conta raiz.

Ação recomendada: inicie sessão na sua conta raiz e ative um dispositivo MFA.

Atividade: Recomendação nº 2

Política de senha do IAM

Descrição: Verifica a política de senhas da conta e alerta quando uma política de senha não está habilitada, ou se os requisitos de conteúdo de senhas não foram ativados. Os requisitos de conteúdo de senhas aumentam a segurança em geral do seu ambiente da AWS com a aplicação da criação de senhas de usuário fortes. Quando você criar ou alterar uma política de senha, a alteração será aplicada imediatamente para novos usuários, mas não forçará os usuários atuais a mudar de senhas.

Critérios de alerta: Uma política de senha está habilitada, mas pelo menos um requisito de conteúdo não está habilitado.

Ação recomendada: se alguns requisitos de conteúdo não estiverem ativados, ative-os. Se nenhuma política de senha estiver habilitada, crie e configure uma. Definição de uma política de senha de contas para usuários do &IAM;

Atividade: Recomendação nº 3

Grupos de segurança – Acesso irrestrito

Descrição: Procura em grupos de segurança por regras que permitem acesso irrestrito a um recurso. O acesso irrestrito aumenta as oportunidades de ação de atividades maliciosas (hacking, ataques de negação de serviço, perda de dados).

Critérios de alerta: Uma regra do grupo de segurança tem um endereço IP de origem com um sufixo /0 para portas que não são 25, 80 ou 443.

Ação recomendada: restrinja o acesso aos endereços IP que exigem isso. Para restringir o acesso a um endereço IP específico, defina o sufixo como /32 (por exemplo, 192.0.2.10/32). Exclua regras excessivamente permissivas depois de criar regras mais restritivas.

Região	Nome do grupo de segurança	ID do grupo de segurança	Protocolo	Porta	Estado	IP Range
us-east-1	WebServerSG	sg-xxxxxxx1 (vpc-xxxxxxx1)	tcp	22	Vermelho	0.0.0.0/0
us-west-2	DatabaseServerSG	sg-xxxxxxx2 (vpc-xxxxxxx2)	tcp	8080	Vermelho	0.0.0.0/0

Atividade: Recomendação nº 4

Snapshots do Amazon EBS

Descrição: Verifica a idade dos snapshots dos volumes (disponíveis ou em uso) do Amazon Elastic Block Store (Amazon EBS). Apesar de os volumes do Amazon EBS serem replicados, falhas podem ocorrer. Os snapshots persistem no Amazon Simple Storage Service (Amazon S3) para garantir armazenamento durável e recuperação point-in-time.

Critérios de alerta:
O snapshot de volume mais recente tem entre 7 e 30 dias.
Vermelho: o snapshot de volume mais recente tem mais de 30 dias.
Vermelho: o volume não tem um snapshot.

Ação recomendada: crie snapshots semanais ou mensais de seus volumes

Região	ID do volume	Nome do volume	ID do snapshot	Nome do snapshot	Idade do snapshot	Anexo de volume	Estado	Motivo
us-east-1	vol-xxxxxxxx	My-EBS-Volume				/dev/...	Vermelho	Não há snapshot

Atividade: Recomendação nº 5

Amazon S3 Bucket Logging
Descrição: verifica a configuração de registro em log dos buckets do Amazon Simple Storage Service (Amazon S3). Quando o registro em log de acesso ao servidor está habilitado, os logs de acesso detalhados são entregues a cada hora em um bucket escolhido. Um registro de log de acesso contém detalhes sobre cada solicitação, como o tipo, os recursos especificados na solicitação e a data e hora em que foi processada. Por padrão, o registro em log de buckets não está habilitado. Você deve habilitar o registro em log se quiser executar auditorias de segurança ou saber mais sobre usuários e padrões de uso.

Critérios de alerta:
Amarelo: O bucket não tem o registro em log de acesso ao servidor habilitado.
Amarelo: As permissões do bucket de destino não incluem a conta do proprietário. O Trusted Advisor não pode verificá-la.

Ação recomendada
Habilite o registro em log de bucket para a maioria dos buckets.
Se as permissões do bucket de destino não incluírem a conta raiz e você quiser que o Trusted Advisor verifique o status do registro em log, adicione a conta do proprietário como um favorecido.

Região	Nome do bucket	Nome do destino	Destino existe	Mesmo proprietário	Gravação habilitada	Motivo
us-east-2	my-hello-world-bucket		Não	Não	Não	Registro em log não habilitado

Principais lições da Seção 3

- O AWS Trusted Advisor é uma ferramenta on-line que fornece orientações em tempo real para ajudar a provisionar recursos de acordo com as melhores práticas da AWS.
- O AWS Trusted Advisor analisa todo o seu ambiente da AWS e oferece recomendações em tempo real em cinco categorias.
- Você pode usar o AWS Trusted Advisor para ajudar a otimizar seu ambiente da AWS assim que começar a implementar seus projetos de arquitetura.

Módulo 9: Arquitetura de nuvem

Conclusão do módulo

aws academy

Resumo do módulo

Resumindo, neste módulo você aprendeu a:

- Descrever o AWS Well-Architected Framework, incluindo os cinco pilares
- Identificar os princípios de design do AWS Well-Architected Framework
- Explicar a importância da confiabilidade e da alta disponibilidade
- Identificar como o AWS Trusted Advisor ajuda os clientes
- Interpretar as recomendações do AWS Trusted Advisor

Conclua o teste de conhecimento

Exemplo de pergunta do exame

Um engenheiro de operações de sistema que trabalha em uma empresa quer proteger seus dados em trânsito e ociosos. Quais serviços ele pode usar para proteger seus dados?

A. Elastic Load Balancing
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon Simple Storage Service (Amazon S3)
D. Todas as opções anteriores

Recursos adicionais

- Site do AWS Well-Architected
- Artigo técnico do AWS Well-Architected Framework
- Laboratórios do AWS Well-Architected
- Verificações de melhores práticas do AWS Trusted Advisor

Obrigado

aws academy