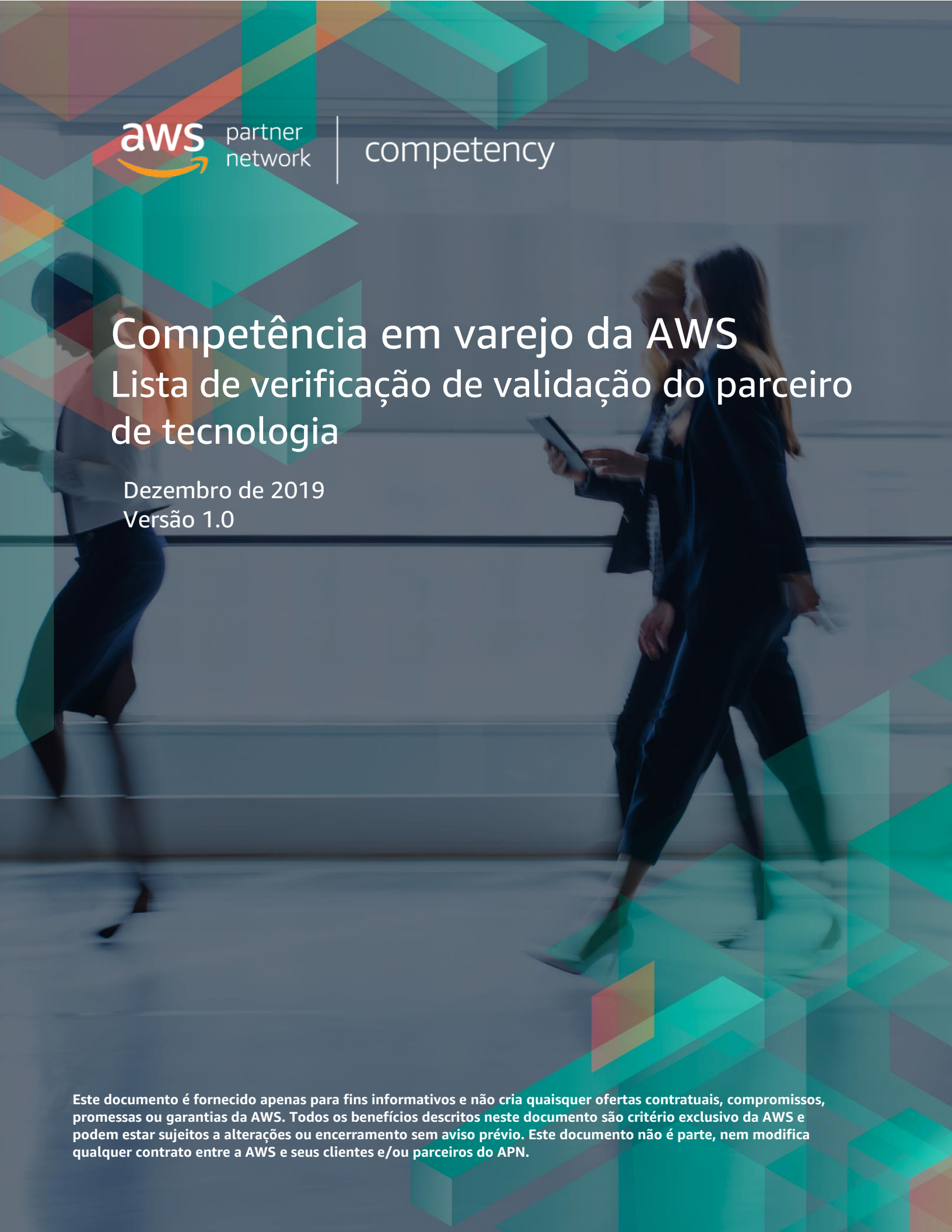

aws partner network | competency

Competência em varejo da AWS
Lista de verificação de validação do parceiro de tecnologia

Dezembro de 2019
Versão 1.0

Índice

Introdução

O objetivo do Programa de competência da AWS é reconhecer os parceiros da Rede de parceiros da AWS (“parceiros do APN”) que demonstram proficiência técnica e histórias de sucesso de clientes comprovadas em áreas de solução especializadas. A Lista de verificação de validação do parceiro de competência (“lista de verificação”) é voltada aos parceiros do APN que têm interesse em se candidatar a uma Competência da AWS. Esta lista de verificação fornece os critérios necessários para participar do Programa de competência da AWS. Os parceiros do APN passam por uma auditoria de suas capacidades quando se candidatam a uma competência específica. A AWS faz uso de sua experiência interna e de uma firma terceirizada para facilitar a auditoria. A AWS se reserva o direito de fazer alterações neste documento a qualquer momento.

Expectativas das partes

É esperado que os parceiros do APN examinem este documento de forma detalhada antes de se candidatarem ao Programa de competência da AWS, mesmo que todos os pré-requisitos sejam atendidos. Se algum item deste documento não estiver claro ou exigir mais explicações, primeiro entre em contato com o Representante de desenvolvimento do parceiro (PDR) ou o Gerente de desenvolvimento do parceiro (PDM) da AWS. Se for necessário obter mais ajuda, o PDR/PDM entrará em contato com o escritório do programa.

Quando estiverem prontos para se candidatar, os parceiros do APN deverão preencher a coluna de autoavaliação do parceiro da lista de verificação definida abaixo neste documento.

Para enviar sua candidatura:

1. Faça login no portal do APN (https://partnercentral.awspartner.com/), como Líder da aliança
2. Selecione “View My APN Account” (Exibir minha conta do APN) no lado esquerdo da página
3. Role até a seção “Program Details” (Detalhes do programa)
4. Selecione “Update” (Atualizar) ao lado da competência da AWS à qual deseja se candidatar
5. Preencha a candidatura ao programa e clique em “Submit” (Enviar)
6. Envie a autoavaliação preenchida para competency-checklist@amazon.com.
    - A autoavaliação deve incluir:
        - A categoria da solução (envolvimento de clientes; comercialização e planejamento corporativos; cadeia de suprimentos e distribuição; loja física, digital e virtual; ciência de dados avançada de varejo aplicativos empresariais essenciais de varejo)
        - O tipo de implantação (SaaS ou implantação pelo cliente na AWS)
        - Documentação para os estudos de caso da AWS (veja as definições a seguir)

Se você tiver alguma dúvida sobre as instruções acima, entre em contato com seu PDR/PDM.
A AWS examinará e tentará responder com eventuais dúvidas em até 5 (cinco) dias úteis para iniciar o agendamento da sua auditoria ou solicitar informações adicionais.

Os parceiros do APN devem se preparar para a auditoria lendo a Lista de verificação, preenchendo uma autoavaliação usando a lista de verificação, reunindo e organizando provas objetivas para compartilhar com o auditor no dia da auditoria.

A AWS recomenda que os parceiros do APN tenham à disposição indivíduos capazes de atestar de maneira detalhada os requisitos durante a auditoria. A melhor prática é que o parceiro do APN disponibilize os seguintes profissionais para a auditoria: um ou mais engenheiros/arquitetos certificados pela AWS altamente técnicos, um engenheiro de operações responsável pelos elementos de operações e suporte e um executivo de desenvolvimento de negócios para conduzir a apresentação de visão geral. Os parceiros do APN devem garantir que têm os consentimentos necessários para compartilhar com o auditor (seja a AWS ou terceiros) todas as informações contidas nas provas objetivas ou em quaisquer demonstrações antes de agendar a auditoria.

Programa de competência em varejo da AWS

Os parceiros de competência em varejo da AWS fornecem soluções de varejo com aplicativos de envolvimento de clientes; comercialização e planejamento corporativos; cadeia de suprimentos e distribuição; loja física, digital e virtual; ciência de dados avançada de varejo e aplicativos empresariais essenciais de varejo.

Categorias de competência em varejo

Os parceiros do APN também devem identificar a categoria do segmento aplicável à sua solução:

- **Envolvimento de clientes:** soluções de fidelidade, gerenciamento de canais sociais, gerenciamento do relacionamento com o cliente (CRM), central de atendimento, publicidade (digital e mala direta), SEO e envolvimento de públicos que permitem que líderes de marketing de varejo atraiam e retenham proativamente os clientes antes e depois da compra.

- **Comercialização e planejamento corporativos:** soluções de comercialização, reabastecimento, planejamentos diversos, planejamento de planogramas e espaços, otimização de promoções e definições de preço, gerenciamento de categorias e colaboração entre fornecedores utilizadas por equipes de comercialização e planejamento corporativas.

- **Cadeia de suprimentos e distribuição:** soluções de cadeia de suprimentos e distribuição abrangendo sistemas de gerenciamento de armazéns (WMS), planejamento de recursos empresariais (ERP), automação de armazéns, importação/exportação, transportes e logística.

- **Loja física, virtual e digital:** soluções que transformam a experiência de compras online e offline, abrangendo pontos de venda, sistemas de gerenciamento de pedidos (OMS), comércio unificado, comércio eletrônico, entrega na última milha, experiência de loja sem limites (sem imprevistos), inovações digitais (AR/VR, ESL, IoT, beacons, voz, reconhecimento quiosque digital, espelhos inteligentes e telas interativas), gerenciamento de ativos digitais (DAM) e pagamentos.

- **Ciência de dados avançada de varejo:** soluções de data lake de varejo, IA/ML e análises que aprimoram a eficiência operacional e os insights e o envolvimento dos clientes.

- **Aplicativos empresariais essenciais de varejo:** soluções corporativas essenciais de varejo para altos executivos e as áreas de finanças, compras, recursos humanos, gerenciamento de funcionários, jurídico e TI.

Os parceiros do APN também devem identificar qual categoria de entrega se aplica à sua solução:

1. **SaaS:** atende a vários clientes usando infraestrutura compartilhada da AWS. Todas as contas da AWS são gerenciadas pelo parceiro do APN.

2. **Implantação pelo cliente:** implantações em um ambiente da AWS do cliente. Todas as contas da AWS são gerenciadas pelo cliente

Pré-requisitos do programa de competência em varejo da AWS

Os itens a seguir serão validados pelo gerente do Programa de competência da AWS. Informações ausentes ou incompletas precisarão ser fornecidas antes que a avaliação de validação de tecnologia seja agendada.

1.0 Associação ao programa do APN		Cumprido S/N
1.1 Nível de parceiro de tecnologia	O parceiro do APN deve ler as diretrizes e definições do programa antes de se inscrever para o Programa de competência em varejo. Clique aqui para obter detalhes do programa	
1.2 Nível de parceiro de tecnologia	É necessário ser um parceiro de tecnologia Advanced do APN antes de se candidatar à competência em varejo da AWS.	
1.3 Categoria da solução	Os parceiros do APN devem identificar a categoria do segmento aplicável à sua solução: ☐ **Envolvimento de clientes** ☐ **Comercialização e planejamento corporativos** ☐ **Cadeia de suprimentos e distribuição** ☐ **Loja física, virtual e digital** ☐ **Ciência de dados avançada de varejo** ☐ **Aplicativos empresariais essenciais de varejo** Os parceiros do APN devem identificar a categoria de entrega aplicável à sua solução: ☐ **SaaS** ☐ **Implantação pelo cliente**	
1.4 Adoção pelos clientes	O parceiro do APN deve descrever o número total de clientes que usam a solução.	

2.0 Estudos de caso		Cumprido S/N
2.1 Estudos de caso específicos de varejo	O parceiro do APN deve ter quatro estudos de caso específicos para uma única solução de varejo sendo analisada. Cada um dos quatro estudos de caso deve estar relacionado a um exemplo de uso da solução do parceiro do APN em uma das seis categorias de segmentos (envolvimento de clientes; comercialização e planejamento corporativos; cadeia de suprimentos e distribuição; loja física, virtual e digital; ciência de dados avançada de varejo e aplicativos empresariais essenciais de varejo. Parceiros do APN com competências em experiência digital do cliente (DCX), dados e análises, IoT, Migração e/ou machine learning da AWS podem reutilizar até quatro estudos de caso de clientes para projetos entregues com soluções altamente direcionadas para resolver desafios setoriais e práticas de consultoria específicos que oferecem um conhecimento de domínio de segmento exclusivo do setor de varejo. Para cada estudo de caso, o parceiro do APN precisa fornecer as seguintes informações: ▪ Nome do cliente ▪ Site do cliente ▪ Desafio do cliente ▪ Como a solução foi implantada para resolver o desafio ▪ Aplicativos ou soluções de terceiros utilizados ▪ Data em que a referência entrou em produção ▪ Resultados ▪ Diagramas de arquitetura, guias de implantação ou outros materiais específicos, dependendo do tipo da solução, conforme descrito na próxima seção. Essas informações serão solicitadas como parte do processo de candidatura do programa na Central de parceiros do APN. As informações fornecidas como parte desse estudo de caso podem ser privadas e não serão divulgadas publicamente. Todos os quatro estudos de caso informados serão examinados na análise de documentação da validação técnica. O estudo de caso não será considerado para a competência se o parceiro do APN não fornecer a documentação necessária para avaliar o estudo de caso em relação a cada item da lista de verificação ou se existirem itens não atendidos na lista de verificação.	

	Os estudos de caso devem descrever implantações executadas nos últimos 18 meses e devem ser de projetos em fase de produção nos clientes e não em fase de piloto ou prova de conceito.	
2.2 Estudos de caso disponíveis ao público	Estudos de caso disponíveis ao público são usados pela AWS após aprovação da competência para demonstrar o sucesso comprovado do parceiro do APN com a solução (com base em KPIs mensuráveis) e para promover a confiança dos clientes de que o parceiro do APN tem a experiência e os conhecimentos necessários para desenvolver e entregar soluções que atendem aos seus objetivos. Das quatro implantações do cliente associadas aos estudos de caso, duas devem ser divulgadas pelo parceiro do APN como estudos de caso disponíveis ao público. Esses estudos de caso podem ser apresentados como estudos de caso formais, whitepapers ou publicações em blogs.	
	Os estudos de caso disponíveis ao público devem ser encontrados facilmente no site do parceiro do APN. Por exemplo, deve ser possível navegar da página inicial do parceiro do APN para o estudo de caso disponível ao público. Além disso, o parceiro do APN deve fornecer links para esses estudos de caso disponíveis ao público no seu aplicativo.	
	Os estudos de caso disponíveis ao público devem incluir o seguinte: ▪ Referências ao nome do cliente, ao nome do parceiro do APN e à AWS ▪ Desafio do cliente ▪ Como a solução foi implantada para resolver o desafio ▪ Como os serviços da AWS foram usados como parte da solução ▪ Resultados	
3.0 Presença na web e liderança de pensamento de varejo da AWS		**Cumprido S/N**
3.1 Página inicial da AWS do parceiro do APN	Uma presença do parceiro do APN na Internet, específica para suas soluções de varejo da AWS, proporciona aos clientes a confiança nos recursos e na experiência em varejo do parceiro do APN. O parceiro do APN deve ter uma página inicial da AWS que descreva sua solução de varejo da AWS, links para casos de uso públicos, listas de parcerias de tecnologia e quaisquer outras informações relevantes que comprovem a experiência do parceiro do APN com varejo e destaquem o trabalho com a AWS. Essa página de varejo específica para a AWS deve ser acessada da página inicial do parceiro do APN. A página inicial em si não é aceitável como página inicial da AWS, a menos que o parceiro do APN seja uma empresa dedicada à tecnologia de varejo e a página inicial reflita o foco do parceiro do APN no varejo.	
3.2 Liderança de pensamento em varejo	Consideramos que os parceiros de competência em varejo da AWS têm especialização no domínio de varejo e desenvolveram soluções inovadoras usando os serviços da AWS. O parceiro do APN deve ter materiais voltados ao público (por exemplo, blogs, artigos impressos, vídeos etc.) demonstrando o foco e a especialização do parceiro do APN em varejo. É necessário fornecer links para exemplos de materiais publicados nos últimos 12 meses.	
4.0 Requisitos empresariais		
4.1 Toolkits prontos para uso em campo	O parceiro do APN tem documentação e toolkits prontos para uso em campo por vendedores, incluindo uma proposição de valor do produto clara que possa ser comunicada à organização de vendas da AWS com todas as informações relevantes necessárias para determinar a adequação a uma oportunidade do cliente (por exemplo, materiais de apoio de vendas, apresentações e casos de uso de clientes). As provas devem estar no formato de material de apoio de vendas, incluindo uma apresentação, um resumo em uma página e uma lista de verificação de caso de uso.	
4.2 Suporte/help desk de produto	O parceiro do APN oferece aos clientes suporte ao produto por meio de chat web, telefone ou e-mail. As provas devem estar no formato de descrição do suporte oferecido aos clientes para o produto ou a solução.	

4.3 Produto anunciado no AWS Marketplace	O parceiro do APN disponibiliza a solução no AWS Marketplace. ☐ Sim ☐ Não Se “sim”, o parceiro do APN deve fornecer um link para o anúncio no AWS Marketplace. Se “não”, nenhuma informação adicional é necessária.	
4.4 Remuneração de vendas para negociações conjuntas da AWS	O parceiro do APN tem planos de remuneração de vendas para seus vendedores em oportunidades conjuntas com a AWS. ☐ Sim ☐ Não ☐ Explique: _____ As provas devem estar no formato de uma breve descrição do plano de remuneração para os vendedores do parceiro do APN.	
4.5 Conquistas conjuntas AWS/parceiro do APN	O parceiro do APN tem um processo para documentar e divulgar conquistas conjuntas. As provas devem ter a forma de uma descrição verbal do processo.	
5.0 Autoavaliação do parceiro do APN		**Cumprido S/N**
5.1 Autoavaliação da lista de verificação de validação do Programa de parceiros de competência da AWS	O parceiro do APN deve conduzir uma autoavaliação quanto à sua conformidade com os requisitos da lista de verificação de validação do parceiro de tecnologia de varejo da AWS. ▪ O parceiro do APN deve preencher todas as seções de lista de verificação. ▪ A autoavaliação preenchida deve ser enviada por e-mail para **competency-checklist@amazon.com** usando a seguinte convenção na linha de assunto do e-mail: “[Nome do parceiro do APN], Retail Competency Technology Partner Completed Self-Assessment”. ▪ Recomendamos que o parceiro do APN solicite que o arquiteto de soluções de parceiros, o representante de desenvolvimento do parceiro (PDR) ou o gerente de desenvolvimento do parceiro (PDM) revise a autoavaliação preenchida antes que ela seja enviada à AWS. O objetivo é garantir que a equipe da AWS do parceiro do APN seja envolvida e trabalhe para fazer recomendações antes da validação, bem como para ajudar a garantir uma experiência de validação positiva.	

Lista de verificação de validação do parceiro de tecnologia de competência em varejo

Os itens a seguir serão validados pelos auditores terceirizados e/ou pelos arquitetos de soluções do parceiro da AWS. Informações ausentes ou incompletas precisarão ser fornecidas antes que a avaliação de validação de tecnologia seja agendada.

Validação técnica		Aplica-se a: SaaS	Aplica-se a: Implantação pelo cliente na AWS	Cumprido S/N
Diagrama de arquitetura	Dependendo da categoria de implantação, um ou mais diagramas de arquitetura são necessários. Cada diagrama de arquitetura deve mostrar: ☐ Os principais elementos da arquitetura e como eles se combinam para fornecer a solução do parceiro aos clientes ☐ Todos os serviços da AWS usados, utilizando os ícones de serviços da AWS adequados. ☐ Como os serviços da AWS são implantados, incluindo a Amazon Virtual Private Cloud (VPC), as zonas de disponibilidade (AZs), as sub-redes e as conexões para sistemas fora da AWS. ☐ Inclui elementos implantados fora da AWS. Por exemplo, componentes ou dispositivos de hardware locais.	Sim. Um para a solução inteira e outro para cada estudo de caso.	Sim. Um para cada estudo de caso.	
Guia de implantação	O guia de implantação deve oferecer as melhores práticas para implantar a solução do parceiro na AWS e inclui todas as seções descritas em "Requisitos de referência para guias de implantação"	Não	Sim. Um para a solução.	
Lista de verificação de validação preenchida	Para cada um dos quatro estudos de caso fornecidos para a solução do parceiro, o parceiro do APN deve fornecer uma versão preenchida da lista de verificação a seguir, indicando os itens da lista de verificação que foram cumpridos.	Sim	Sim	
1.0 Segurança **O foco do pilar de segurança é a proteção de informações e sistemas. Os tópicos principais incluem a confidencialidade e a integridade de dados, a identificação e o gerenciamento das atividades que podem ser realizadas pelos usuários com o gerenciamento de privilégios, a proteção de sistemas e o estabelecimento de controles para detectar eventos de segurança.**				
1.1 Usuário raiz da conta da AWS não é usado para atividades de rotina	O usuário raiz da conta da AWS não deve ser usado para atividades de rotina. Imediatamente após a criação da sua conta da AWS, você deve criar contas de usuários do AWS Identity and Access Management (IAM) e usar essas contas de usuários do IAM para todas as atividades de rotina. Após a criação das contas de usuários do IAM, você deve guardar as credenciais da conta raiz da AWS em lugar seguro e usá-las apenas para executar as poucas tarefas de gerenciamento de contas e serviços que exigem o usuário raiz da conta da AWS. Para obter mais informações sobre como configurar contas e grupos de usuários do IAM para uso diário, consulte Criação de seu primeiro usuário administrador e grupo do IAM.	Sim	Não	
1.2 Multi-Factor Authentication (MFA) foi habilitada no usuário raiz da conta da AWS	A Multi-Factor Authentication (MFA) deve ser habilitada no usuário raiz da conta da AWS. Como o usuário raiz da conta da AWS pode executar operações delicadas na conta da AWS, a adição de uma camada adicional de autenticação ajuda a proteger melhor a conta. Vários tipos de MFA estão disponíveis, incluindo MFA virtual e MFA por hardware.	Sim	Não	
1.3 Contas de usuário do IAM usadas para todas as atividades de rotina	O usuário raiz da conta da AWS não deve ser usado em nenhuma tarefa em que não seja obrigatório. Em vez disso, crie um novo usuário do IAM para cada pessoa que exige acesso de administrador. Em seguida, converta esses usuários em administradores colocando-os no grupo Administradores ao qual você anexou a política gerenciada Acesso de administradores. A partir desse momento, os usuários dos grupos de administradores devem configurar os grupos, os usuários e outras definições da conta da AWS. Todas as interações futuras devem ocorrer por meio dos usuários das contas da AWS e de	Sim	Não	

	suas próprias chaves, em vez do usuário raiz. No entanto, para executar algumas tarefas de gerenciamento de contas e serviços, você deve fazer login usando as credenciais do usuário raiz.			
1.4 Multi-Factor Authentication (MFA) está habilitada para todos os usuários interativos do IAM	Você deve habilitar a MFA para todos os usuários interativos do IAM. Com o MFA, os usuários têm um dispositivo que gera um código de autenticação único, ou One-Time Password (OTP – Senha de uso único). Os usuários devem fornecer suas credenciais normais (nome do usuário e senha) e a OTP. O dispositivo MFA pode ser um hardware específico ou um dispositivo virtual (por exemplo, pode ser um aplicativo executado em um smartphone).	Sim	Não	
1.5 Credenciais do IAM são alternadas regularmente	Você deve alterar as senhas e chaves de acesso regularmente e assegurar que todos os usuários do IAM na sua conta façam o mesmo. Dessa forma, se uma senha ou chave de acesso for comprometida sem que você perceba, o período de uso das credenciais para acessar recursos é limitado. Você pode aplicar uma política de senhas na conta para exigir que todos os usuários do IAM alternem suas senhas e especificar a frequência com que isso deve ser feito. Para obter mais informações sobre a alternância de chaves de acesso para usuários do IAM, consulte Mudança das chave de acesso.	Sim	Não	
1.6 Política de senhas robusta implementada para usuários do IAM	Você deve configurar uma política de senhas robusta para os usuários do IAM. Se você permitir que os usuários alterem suas próprias senhas, exija que eles criem senhas fortes e que as alternem periodicamente. Na página Account Settings do console do IAM, você pode criar uma política de senhas para a sua conta. A política de senhas pode ser usada para definir requisitos de senha como comprimento mínimo, obrigatoriedade de caracteres não alfabéticos, frequência da alternância e assim por diante. Para obter mais informações, consulte Definição de uma política de senhas de contas para usuários do IAM.	Sim	Não	
1.7 Credenciais do IAM não são compartilhadas entre vários usuários	Você deve criar uma conta de usuário do IAM individual para qualquer pessoa que precise acessar a sua conta da AWS. Crie também um usuário do IAM para você, atribua privilégios administrativos a esse usuário e use esse usuário do IAM para fazer todo o seu trabalho. A criação de usuários do IAM individuais para as pessoas que acessam a sua conta permite que cada usuário do IAM receba um conjunto único de credenciais de segurança. Você também pode conceder permissões diferentes para cada usuário do IAM. Se necessário, você pode alterar ou revogar as permissões do usuário do IAM a qualquer momento. (Se você distribuir as credenciais do usuário raiz, será difícil revogá-las e impossível restringir suas permissões.)	Sim	Não	
1.8 Escopo de políticas do IAM é reduzido para o menor privilégio	Você deve seguir a orientação padrão de segurança de conceder o menor privilégio possível. Isso significa conceder apenas as permissões necessárias para executar uma tarefa. Determine o que os usuários precisam fazer e crie políticas para eles que permitem apenas a execução dessas tarefas. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme a necessidade. Esse procedimento é mais seguro que começar com permissões abrangentes demais e depois tentar reduzi-las. Para definir o conjunto correto de permissões, é necessária alguma pesquisa. Determine o que é necessário para a tarefa específica, quais ações são permitidas por um determinado serviço e que permissões são necessárias para executar essas ações.	Sim	Não	
1.9 Credenciais definidas no código (por exemplo, chaves de acesso) não são usadas	Você deve seguir as melhores práticas para gerenciar chaves de acesso da AWS e evitar o uso de credenciais definidas no código. Quando você acessa a AWS de forma programática, pode usar uma chave de acesso para verificar a sua identidade e a dos aplicativos. Qualquer pessoa que tenha a sua chave de acesso terá um nível de acesso aos recursos da AWS idêntico ao seu. Portanto, a AWS se esforça para proteger as suas chaves de acesso e, de acordo com o nosso modelo de responsabilidade compartilhada, você deve fazer o mesmo.	Sim	Sim	

1.10 Todas as credenciais ociosas são criptografadas	O requisito de referência é garantir a criptografia de todas as credenciais ociosas.	Sim	Sim	
1.11 Chaves de acesso da AWS usadas apenas por usuários interativos	Nenhuma chave de acesso da AWS deve ser usada, exceto nestes casos: 1. Uso por uma pessoa para acessar serviços da AWS e armazenada de forma segura em um dispositivo controlado por essa pessoa. 2. Uso por um serviço para acessar serviços da AWS, mas apenas quando a) não é viável usar uma função de instância do Amazon EC2, uma função de tarefa do Amazon Elastic Container Service (Amazon ECS) ou um mecanismo semelhante; b) as chaves de acesso da AWS são alternadas pelo menos uma vez por semana e c) o escopo da política do IAM é reduzido para: i) somente permitir acesso a métodos e destinos específicos e ii) restringir o acesso às sub-redes em que os recursos serão acessados.	Sim	Sim	
1.12 O AWS CloudTrail está habilitado para todas as contas da AWS em cada região	O AWS CloudTrail deve estar habilitado em todas as contas da AWS e em todas as regiões. A visibilidade da atividade da conta da AWS é um aspecto essencial das melhores práticas de segurança e operações. Você pode usar o AWS CloudTrail para ver, pesquisar, fazer download, arquivar, analisar e responder à atividade da conta em toda a infraestrutura da AWS. É possível identificar quem ou o que executou qual ação, quais recursos foram afetados, quando o evento ocorreu e outros detalhes que ajudam a analisar e responder à atividade da conta da AWS.	Sim	Não	
1.13 Logs do CloudTrail são armazenados em um bucket do S3 de propriedade de outra conta da AWS	Os logs do AWS CloudTrail devem estar em um bucket de propriedade de outra conta da AWS, configurada para acesso extremamente limitado, como somente auditoria e recuperação.	Sim	Não	
1.14 Versionamento ou exclusão com MFA deve estar habilitado no bucket do S3 que armazena os logs do CloudTrail	O conteúdo do bucket de logs do AWS CloudTrail deve estar protegido por versionamento ou exclusão com MFA.	Sim	Não	
1.15 Escopo de grupos de segurança do Amazon EC2 é reduzido	Todos os grupos de segurança do Amazon EC2 devem restringir o acesso ao mínimo possível. Isso inclui pelo menos 1. Implementação de grupos de segurança para restringir o tráfego entre a Internet e a Amazon VPC; 2. Implementação de grupos de segurança para restringir o tráfego dentro da Amazon VPC e 3. Em todos os casos, permitir apenas as configurações com a maior restrição possível.	Sim	Sim	
1.16 Buckets do Amazon S3 nas suas contas têm níveis de acesso adequados	Você deve garantir a implementação de controles adequados para controlar o acesso a cada bucket do Amazon S3. Uma melhor prática ao usar a AWS é restringir o acesso aos recursos às pessoas que realmente precisam deles (o princípio do menor privilégio possível).	Sim	Sim	
1.17 Buckets do Amazon S3 não foram configurados indevidamente para permitir acesso público.	Você deve garantir que todos os buckets que não devem permitir acesso público sejam configurados adequadamente para evitar o acesso público. Por padrão, todos os buckets do Amazon S3 são privados e somente podem ser acessados por usuários que receberam explicitamente esse acesso. A maioria dos casos de uso não exige acesso público amplo para ler arquivos de buckets do Amazon S3, a menos que você use o Amazon S3 para hospedar ativos públicos (por exemplo, imagens para uso em um site público). A melhor prática é nunca conceder acesso ao público.	Sim	Sim	
1.18 Mecanismo de monitoramento implementado	Você deve implementar monitoramento ou alertas para identificar quando os buckets do Amazon S3 se tornam públicos. Uma opção para fazer isso é usar o AWS Trusted Advisor. O AWS	Sim	Não	

para detectar quando buckets ou objetos do S3 se tornam públicos	Trusted Advisor verifica os buckets do Amazon S3 que têm permissões de acesso aberto. As permissões de bucket que concedem acesso de listagem a todos poderão resultar em custos superiores aos esperados se os objetos do bucket forem acessados por usuários indesejados com alta frequência. As permissões de bucket que concedem acesso de upload/exclusão a todos criam possíveis vulnerabilidades de segurança, pois permitem que qualquer pessoa adiciona, modifique ou remova itens em um bucket. A verificação do Trusted Advisor examina as permissões de bucket explícitas e as políticas de bucket associadas que podem substituir as permissões de bucket.			
1.19 Mecanismo de monitoramento implementado para detectar alterações em instâncias e contêineres do Amazon EC2	Todas as alterações efetuadas em instâncias ou contêineres do Amazon S3 podem indicar atividade não autorizada e, no mínimo, devem ser registradas em log em um local resiliente para permitir futuras investigações forenses. O mecanismo utilizado para essa finalidade deve, no mínimo: 1. Detectar todas as alterações em arquivos do SO ou dos aplicativos nas instâncias ou contêineres do Amazon S3 usados na solução. 2. Armazenar os dados que registram essas alterações em um local resiliente, externo à instância e ao contêiner do Amazon S3. Entre os exemplos de mecanismos adequados, estão: a. implantação de verificação de integridade de arquivos por meio de gerenciamento de configuração agendado (por exemplo, Chef, Puppet etc.) ou ferramenta especializada (por exemplo, OSSEC, Tripwire ou semelhante) ou b. Estender as ferramentas de gerenciamento de configuração para validar a configuração do host do Amazon S3 e alertar em caso de atualizações em arquivos de configuração chave ou pacotes com eventos “canary” (no-op registrados em log) configurados para assegurar que o serviço continue operacional em todos os hosts no escopo durante o tempo de execução ou c. implantar um sistema de detecção de invasões de host (por exemplo, uma solução de código aberto como OSSEC com Elasticsearch e Kibana) ou usando uma solução de parceiros. Observe que o mecanismo a seguir não cumpre esse requisito: a. Desativação/ativação frequentes de instâncias ou contêineres do Amazon S3.	Sim	Não	
1.20 Todos os dados são classificados	Todos os dados do cliente processados e armazenados na carga de trabalho são considerados e classificados para determinar sua confidencialidade e os métodos adequados a serem usados durante o processamento desses dados.	Sim	Sim	
1.21 Todos os dados confidenciais são criptografados	Todos os dados do cliente classificados como confidenciais são criptografados quando ociosos e em trânsito.	Sim	Sim	
1.22 As chaves criptográficas são gerenciadas de forma segura	Todas as chaves criptográficas são criptografadas quando ociosas e em trânsito. O acesso para uso das chaves é controlado usando uma solução da AWS como o AWS Key Management Service (KMS) ou uma solução de parceiros como o HashiCorp Vault.	Sim	Sim	
1.23 Todos os dados em trânsito são criptografados	Todos os dados em trânsito entre limites de Amazon Virtual Private Clouds são criptografados.	Sim	Sim	
1.24 Processo de resposta a incidentes definido e ensaiado	Um processo de resposta a incidentes de segurança deve ser definido para lidar com incidentes como comprometimento de uma conta da AWS. Esse processo deve ser testado pela implementação de procedimentos para ensaiar o processo de resposta a incidentes. Por exemplo, a realização de um exercício com simulações de segurança. Um ensaio deve ter sido realizado nos últimos 12 meses para confirmar que: a. as pessoas apropriadas têm acesso ao ambiente. b. as ferramentas adequadas estão disponíveis. c. as pessoas apropriadas sabem o que fazer para responder aos diversos incidentes de segurança descritos no plano.	Sim	Não	

1.25 Payment Card Industry Data Security Standard (PCI DSS – Padrão de segurança de dados do setor de cartões de pagamento) – Certificação ou SAQ	Para aplicativos de comércio eletrônico, comércio unificado e pontos de venda, que contam com a presença física do titular do cartão, é estabelecido um processo para executar uma avaliação anual do escopo do Payment Card Industry Data Security Standard (PCI DSS) para a carga de trabalho. De acordo com a avaliação de escopo, a certificação ou o SAQ do PCI DSS são executados conforme a necessidade. As provas devem estar no formato de um relatório de conformidade para certificação do PCI DSS ou de um questionário de autoavaliação (SAQ).	Sim	Sim	
1.26 Criptografia completa de dados do PCI	Para aplicativos de comércio eletrônico, comércio unificado e pontos de venda, que contam com a presença física do titular do cartão, os dados são criptografados em trânsito mesmo dentro de uma Amazon VPC.	Sim	Sim	
1.27 Proteção contra ataques de negação distribuída de serviços (DDoS) implementada	Fornece infraestrutura e serviços que mitigam ataques de negação distribuída de serviços (DDoS) em todas as camadas do modelo Open Systems Interconnection (OSI).	Sim	Não	
1.28 Mecanismos implementados para mitigar os principais 10 ataques do Open Web Application Security Project (OWASP)	Fornece infraestrutura e serviços que mitigam vulnerabilidades do Open Web Application Security Project (OWASP).	Sim	Não	
2.0 Confiabilidade O foco do pilar da confiabilidade é a capacidade de evitar e recuperar-se rapidamente de falhas no atendimento a demandas empresariais e do cliente. Os principais tópicos incluem elementos fundamentais de configuração, requisitos para vários projetos relacionados, planejamento de recuperação e a forma de lidar com mudanças.				
2.1 Conectividade de rede altamente disponível	A conectividade de rede para a solução deve estar altamente disponível. Se você usar VPN ou o AWS Direct Connect para conectar-se a redes do cliente, a solução deverá oferecer suporte a conexões redundantes, mesmo que o cliente nem sempre implemente esse recurso.	Sim	Sim	
2.2 Mecanismos de escalabilidade de infraestrutura alinhados a requisitos empresariais	Mecanismos de escalabilidade de infraestrutura devem estar alinhados a requisitos empresariais de uma das seguintes formas: 1. Implementação de mecanismos de escalabilidade automática em cada camada da arquitetura ou 2. Confirmação de que os requisitos empresariais atuais, incluindo requisitos de custo e crescimento estimado de usuários, não exigem mecanismos de escalabilidade automática E de que os procedimentos de escalabilidade manual estão totalmente documentados e são testados com frequência.	Sim	Sim	
2.3 Gerenciamento centralizado de logs da AWS e dos aplicativos	Todas as informações de log do aplicativo e da infraestrutura da AWS devem ser consolidadas em um único sistema.	Sim	Não	
2.4 Gerenciamento centralizado de monitoramento e alarmes da AWS e dos aplicativos	O aplicativo e a infraestrutura da AWS devem ser monitorados de forma centralizada, com geração e envio de alarmes à equipe de operações apropriada.	Sim	Não	
2.5 Provisionamento e gerenciamento automatizados de infraestrutura	A solução deve usar uma ferramenta automatizada como o AWS CloudFormation ou o Terraform para provisionar e gerenciar a infraestrutura da AWS. O Console AWS não deve ser usado para fazer alterações de rotinas na infraestrutura de produção da AWS.	Sim	Sim	

2.6 Backups de dados regulares são executados	Você deve executar backups regulares para um serviços de armazenamento resiliente. Os backups asseguram a sua capacidade de recuperação em cenários de erros administrativos, lógicos ou físicos. O Amazon S3 e o Amazon Glacier são serviços ideais para backup e arquivamento. Ambos são plataformas de armazenamento resilientes e de baixo custo. Ambos oferecem capacidade ilimitada e não exigem gerenciamento de volumes ou mídia à medida que os conjuntos de dados de backup crescem. O modelo de pagamento conforme o uso e o baixo custo por GB/mês tornam esses serviços uma boa opção para casos de uso de proteção de dados.	Sim	Sim	
2.7 Mecanismos de recuperação são testados regularmente e após alterações de arquitetura significativas	Você deve testar mecanismos e procedimentos de recuperação periodicamente e após alterações significativas no seu ambiente de nuvem. A AWS fornece recursos substanciais para ajudar você a gerenciar o backup e a restauração dos seus dados.	Sim	Não	
2.8 Solução resiliente a interrupções das zonas de disponibilidade	A solução deve continuar a operar caso todos os serviços de uma única zona de disponibilidade sejam interrompidos.	Sim	Sim	
2.9 Resiliência da solução foi testada	A resiliência da infraestrutura a interrupções de uma única zona de disponibilidade foi testada em produção (por exemplo, por meio de um exercício de simulação) nos últimos 12 meses.	Sim	Não	
2.10 Plano de Disaster Recovery (DR – Recuperação de desastres) foi definido	Um plano de recuperação de desastres bem definido inclui um Recovery Point Objective (RPO – Objetivo de ponto de recuperação) e um Recovery Time Objective (RTO – Objetivo de tempo de recuperação). Você deve definir um RPO e um RTO para todos os serviços no escopo, e o RPO e o RTO devem estar alinhados ao SLA oferecido aos seus clientes.	Sim	Sim	
2.11 Recovery Time Objective (RTO – Objetivo de tempo de recuperação) é inferior a 24 horas	O requisito de referência é que o RTO seja inferior a 24 horas para os serviços essenciais.	Sim	Não	
2.12 Plano de recuperação de desastres (DR) foi testado adequadamente	O plano de recuperação de desastres deve ser testado em relação ao RPO e ao RTO periodicamente e após atualizações importantes. Pelo menos um teste de recuperação de desastres deve ser concluído antes da aprovação da sua candidatura ao nível Advanced do APN da AWS.	Sim	Não	
2.13 Plano de recuperação de desastres (DR) inclui a recuperação para outra região	O plano de recuperação de desastres deve incluir uma estratégia de recuperação para outra região da AWS e o teste periódico de recuperação deve testar esse cenário. Você deve ter concluído pelo menos um teste completo do plano de recuperação de desastres, incluindo pelo menos a recuperação para outra região da AWS, nos últimos 12 meses. Observação: embora processos que restauram dados para ambientes de teste ou exportam dados para os usuários sejam formas úteis de verificar backups, esses processos não cumprem o requisito de executar um teste completo de restauração para outra região da AWS.	Sim	Não	
3.0 Excelência operacional O foco do pilar de excelência operacional é a execução e o monitoramento de sistemas para entregar valor empresarial e a melhoria contínua de processos e procedimentos. Os principais tópicos incluem o gerenciamento e a automatização de alterações, a resposta a eventos e a definição de padrões para gerenciar de forma bem-sucedida as operações diárias.				
3.1 Implantação automatizada de alterações de código	A solução deve usar um método automatizado de implantação de código na infraestrutura da AWS. Sessões interativas do Secure Shell (SSH) ou do Remote Desktop Protocol (RDP) não devem ser usadas para implantar atualizações na infraestrutura da AWS.	Sim	Não	

3.2 Runbooks e processos de encaminhamento definidos	Runbooks devem ser desenvolvidos para definir os procedimentos padrão usados em resposta a diferentes eventos de aplicativos e da AWS. Um processo de encaminhamento deve ser definido para lidar com alertas e alarmes gerados pelo sistema e para responder a incidentes relatados pelo cliente. O processo de encaminhamento também deve incluir o encaminhamento ao AWS Support, quando for o caso.	Sim	Não	
3.3 AWS Business Support está habilitado para a conta da AWS	O Business Support deve estar habilitado. O Business Support (ou superior) é um requisito da rede de parceiros da AWS para parceiros de tecnologia no nível Advanced. Para se qualificar para o nível Advanced, você deve habilitar o Business Support em pelo menos uma das suas contas da AWS.	Sim	Não	
4.0 Eficiência da performance O foco do pilar de eficiência de performance é o uso eficiente dos recursos de eficiência e TI. Os tópicos principais incluem a seleção dos tipos e tamanhos de recursos corretos com base nos requisitos de carga de trabalho, o monitoramento da performance e a tomada de decisões informadas para manter a eficiência para acompanhar a evolução das necessidades empresariais.				
4.1 Teste de performance habilitado após as implantações	Defina metas de performance mensuráveis e teste a performance para verificar o cumprimento das metas de performance antes da implantação em produção.	Sim	Sim	
4.2 Limites de monitoramento implementados	Monitore a performance de aplicativos e implemente mecanismos para acionar alarmes quando limites são excedidos.	Sim	Sim	

Recursos da AWS:

Cargo	Descrição
Como criar uma página de destino de prática	Fornece orientação sobre como criar uma página de prática/ solução que atenderá aos pré-requisitos do programa.
Como escrever um estudo de caso público	Fornece orientação sobre como criar um estudo de caso de cliente público que atenderá aos pré-requisitos do programa.
Como criar um diagrama de arquitetura	Fornece orientação sobre como criar diagramas de arquitetura que atenderão aos pré-requisitos do programa.
Documento de prontidão do parceiro	Fornece exemplos de orientação e melhores práticas dos pré-requisitos do programa.
Site do AWS Well Architected	Cobre as melhores práticas do Well Architected