Competência em cargas de trabalho da Microsoft na AWS

Lista de verificação de validação do parceiro de tecnologia

Junho de 2019

Versão 1.0

aws partner network

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 (projeto de produto, projeto de produção, produção ou operações)
        - O tipo de implantação (SaaS ou Customer Deployed on 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 a programação 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 sócios 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.

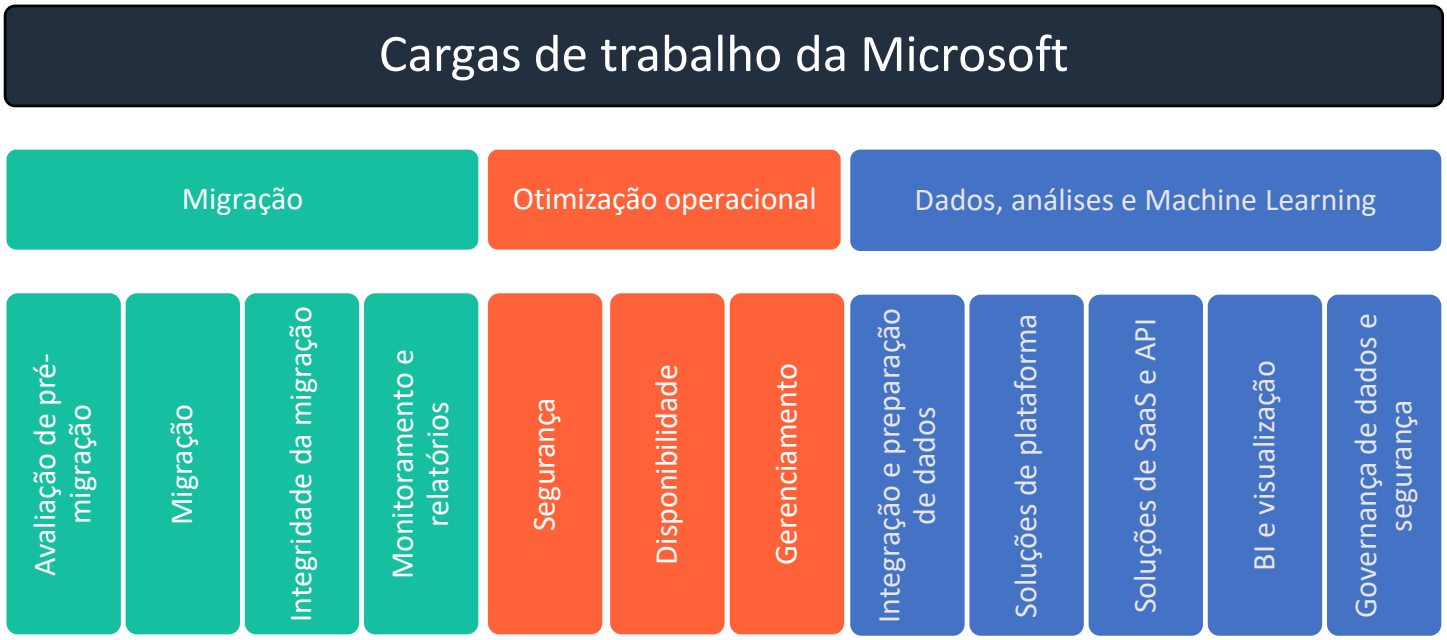
Programa de competência em cargas de trabalho da Microsoft na AWS

Este Programa de competência em cargas de trabalho da Microsoft na AWS (chamado de "Competência em cargas de trabalho da Microsoft na AWS" ou "Competência") identifica e valida as ofertas dos Parceiros de tecnologia do APN que ajudam os clientes a avaliar e migrar cargas de trabalho da Microsoft para a AWS, além de implantar, otimizar e modernizar as cargas de trabalho da Microsoft na AWS. As ofertas relevantes são segmentadas em três categorias: Migração, Otimização operacional e Dados/Análise/Machine Learning Essas categorias são divididas em subcategorias de funcionalidade. Os parceiros do APN podem solicitar e ingressar no programa Competências da AWS por meio de uma ou mais categorias.

Categorias de competência em cargas de trabalho da Microsoft na AWS

Os parceiros do APN também devem identificar a categoria e a subcategoria (ou categorias) do segmento aplicável à sua solução:

1. **Migração de cargas de trabalho da Microsoft**: as tecnologias nesta categoria fornecem avaliação e planejamento pré-migração ou automatização e gerenciamento da migração de cargas de trabalho da Microsoft.
2. **Otimização operacional**: as tecnologias nessa categoria são usadas para otimizar e automatizar as cargas de trabalho da Microsoft na AWS nas áreas que incluem segurança, disponibilidade e gerenciabilidade.
3. **Dados, Análise e Machine Learning:** as tecnologias dessa categoria preparam, transformam, analisam e controlam os dados do Microsoft SQL Server com o objetivo de análise de dados e machine learning na AWS.



Esta tabela foi modificada

Pré-requisitos do programa de competência em cargas de trabalho da Microsoft na 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 programada.

1.0 Requisitos do programa do APN		**Cumprido S/N**
1.1 Diretrizes do programa	O parceiro do APN deve ler as diretrizes e definições do programa antes de se inscrever para o Programa de competência em cargas de trabalho da Microsoft. Clique aqui para obter detalhes do programa.	
1.2 Nível de parceiros de tecnologia do APN	O parceiro do APN deve ser um parceiro de tecnologia do APN de nível Advanced	
1.3 Categoria da solução	O parceiro do APN deve identificar a categoria e a subcategoria (ou subcategorias) do segmento para sua solução. Categoria: ▪ **Migração de cargas de trabalho da Microsoft** ☐ Avaliação de pré-migração ☐ Aplicativo e migração de dados ☐ Integridade da migração ☐ Monitoramento e relatórios ▪ **Otimização operacional das cargas de trabalho da Microsoft** ☐ Gerenciamento de segurança e ameaças ☐ Disponibilidade e recuperação de desastres ☐ Gerenciamento de Recursos, Inventário/Integridade/Monitoramento de custos e relatórios, Gerenciamento de recursos, Inventário/Integridade/Monitoramento de custos e relatórios ▪ **Dados, análise e Machine Learning para cargas de trabalho da Microsoft** ☐ Integração e preparação de dados ☐ Soluções de plataforma ☐ Soluções de SaaS e API ☐ Business Intelligence e visualização ☐ Governança de dados, conformidade e segurança	
2.0 Estudos de caso		**Cumprido S/N**
2.1 Estudos de caso específicos de carga de trabalho da Microsoft	O parceiro do APN deve ter um mínimo de quatro (4) estudos de caso que demonstrem o uso de tecnologia do parceiro do APN correspondente à categoria em análise. No caso de parceiros do APN já validados nas competências de migração, DevOps ou dados e análise da AWS, a solicitação é reduzida ao mínimo de 2 casos de estudo, um público e outro privado, que demonstre o uso da tecnologia do parceiro do APN com as cargas de trabalho da Microsoft correspondentes à categoria em análise. Se mais de uma categoria estiver em análise, pelo menos um estudo de caso deve demonstrar o uso da tecnologia em cada subcategoria. Para cada estudo de caso, o parceiro do APN precisa fornecer as seguintes informações: ▪ Nome 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. Todos os quatro estudos de caso informados serão examinados na validação técnica. O estudo de caso não será considerado para a Competência da AWS se o parceiro do APN não fornecer a documentação necessária para conferir o estudo de caso em relação a cada item da lista de verificação ou se qualquer item na lista de verificação não for atendido. Os estudos de caso devem descrever implantações executadas nos últimos 18 meses e ser de projetos em fase de produção com os clientes, e não em fase piloto ou prova de conceito.	
2.2 Estudos de caso públicos	Os 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 Indicadores chave de performance (KPIs) mensuráveis e fornecer aos clientes a confiança de que o Parceiro do APN possui a tecnologia para atingir seus objetivos. Das quatro (4) implantações do cliente associadas aos estudos de caso, duas (2) 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, vídeos 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: ▪ Nome do cliente, nome do parceiro do APN e a 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 cargas de trabalho da Microsoft na AWS		**Cumprido S/N**
3.1 Microsite parceiro da AWS	Uma presença do parceiro do APN na Internet específica para suas soluções de cargas de trabalho da microsoft na AWS dá aos clientes confiança nas capacidades e na experiência do parceiro do APN. O parceiro do APN deve ter uma página de microsite da AWS que descreva sua solução de cargas de trabalho da Microsoft na AWS, links aos estudos de caso disponíveis ao público, listas de parcerias de tecnologia e quaisquer outras informações relevantes que comprovem a experiência do parceiro com cargas de trabalho da Microsoft e destaquem a parceria com a AWS. Esse microsite de cargas de trabalho da Microsoft específico da AWS deve ser acessado da página inicial do parceiro do APN. A página inicial em si não é aceitável como microsite da AWS, a menos que o parceiro do APN seja uma empresa dedicada às cargas de trabalho da Microsoft e a página inicial reflita o foco do parceiro do APN nas cargas de trabalho da Microsoft.	
3.2 Liderança de pensamento de cargas de trabalho da Microsoft	Consideramos que os parceiros de competência em cargas de trabalho da Microsoft da AWS têm especialização no domínio de gerenciamento da nuvem e desenvolveram soluções inovadoras que usam ou ajudam a gerenciar os serviços da AWS. O parceiro do APN deve ter materiais voltados ao público (por exemplo, publicações de blog, artigos impressos, vídeos etc.) demonstrando o foco e a especialização do parceiro do APN em cargas de trabalho da Microsoft. É necessário fornecer links para exemplos de materiais publicados nos últimos 12 meses.	
4.0 Requisitos empresariais		**Cumprido S/N**
4.1 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 na forma de descrição do suporte oferecido aos clientes para o produto ou a solução.	
4.2 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. O AWS Marketplace não é obrigatório para alcançar a competência.	
4.3 Modelo de implantação	O parceiro do APN identifica todas as opções de modelo de implantação disponíveis aos clientes. ☐ SaaS na AWS ☐ SaaS fora da AWS (para migração) ☐ BYOL na AWS ☐ BYOL em ambiente local (para migração)	
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 de conformidade com essa lista de verificação. ▪ O parceiro do APN deve preencher todas as seções da 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], Microsoft Workloads Competency Technology Partner Completed Self-Assessment”. ▪ Recomendamos que o parceiro do APN solicite que o arquiteto de soluções de parceiros, o PDR ou o 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.	

Pré-requisitos de validação do programa de competência em cargas de trabalho da Microsoft na AWS

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

Requisitos técnicos das cargas de trabalho da Microsoft por categoria

Uma documentação que descreve como a solução do parceiro do APN cumpre os requisitos deve ser enviada como parte da autoavaliação da competência da AWS.

Migração de cargas de trabalho da Microsoft

Recursos obrigatórios da solução		Cumprido S/N
Avaliação de pré-migração	A solução de tecnologia deve usar tecnologia de agente ou sem agente para identificar automaticamente as cargas de trabalho que serão migradas para a AWS. Isso pode incluir: ▪ Avaliação de pré-migração da carga de trabalho da Microsoft dentre uma (ou mais) destas opções: o Avaliação de servidores e máquinas virtuais que executam o Microsoft Windows no ambiente local o Avaliação do contêiner do docker (em execução no Windows Server ou se o contêiner estiver executando o aplicativo .NET/.NET Core) o Avaliação do aplicativo .NET/.NET Core o Avaliação de migração de dados (SQL, sistema de arquivo, blob etc.) o Avaliação de migração de soluções corporativas (Active Directory, OneDrive, Dynamics, Exchange etc.). ▪ O relatório de avaliação de pré-migração deve ser gerado. cada carga de trabalho no grupo de recursos da AWS designado pelo cliente	
Migração	A solução de tecnologia deve usar tecnologia de agente ou sem agente para migrar automaticamente as cargas de trabalho identificadas para a AWS ou dados como parte da migração da carga de trabalho. Isso pode incluir: ▪ Migração de carga de trabalho da Microsoft de uma das seguintes opções: o Migração de máquinas virtuais o Migração do contêiner do docker (em execução no Windows Server ou se o contêiner estiver executando o aplicativo .NET/.NET Core) o Migração do aplicativo .NET/.NET Core o Migração de dados (SQL, sistema de arquivo, blob etc.) o Migração de soluções corporativas (Active Directory, OneDrive, Dynamics, Exchange etc.). ▪ Capacidade de executar backup e reversão no caso de qualquer fase da migração ser malsucedida, a qualquer momento, com perda mínima ou nula de dados. ▪ Permissão para configurações de nuvem híbrida para recuperação de desastres ▪ Diferença de sincronização delta para sincronizar dados após a migração até o corte e o servidor/instância de origem ser desligado. ▪ Corte de cada carga de trabalho no grupo de recursos da AWS designado pelo cliente	
Integridade da migração	A solução de tecnologia deve fazer uma avaliação durante a migração para verificar em tempo real: ▪ Integridade de dados ▪ Integridade do aplicativo	

	▪ Avaliação geral da integridade da arquitetura conectada	
Monitoramento e relatórios	A solução de tecnologia deve incluir: ▪ Monitoramento de processo da migração ▪ Notificações, avisos e relatórios de erros ▪ Relatório geral de migração	

Otimização operacional

Recursos obrigatórios da solução		**Cumprido S/N**
Segurança	A solução de tecnologia deve realizar uma das opções a seguir: ▪ Configuração da postura de segurança (acesso baseado em função, acesso e gerenciamento de identidade, configuração de proxy/firewall, roteamento, criptografia etc.) ▪ Análise de DLP (Prevenção contra perda de dados) ▪ Postura de segurança de rede e instância (portas/certificados/configuração de segurança) ▪ Modelagem de ameaças para tráfego de rede (possíveis vetores de ataque) e alertas. ▪ Conformidade (HIPAA, PCI, SOX etc.) ▪ Capacidade de recomendar melhorias na postura de segurança ▪ Verificação de código-fonte para más práticas, vazamentos de memória, higiene de dados e problemas de segurança.	
Disponibilidade	A solução de tecnologia deve realizar uma das opções a seguir: ▪ Verificação contínua de recuperação de desastres. (Mecanismo de caos) o Escalabilidade o Disponibilidade o Integridade e resiliência de dados ▪ Análise de recursos para determinar problemas de alta disponibilidade. ▪ Capacidade de escalonamento automático (reduzir e aumentar) à medida que a carga de trabalho varia	
Gerenciamento	A solução de tecnologia deve realizar uma das opções a seguir: ▪ Listagem e análise de inventário (em instâncias do Amazon EC2, contêineres, sem servidor) de: o Ativos de carga de trabalho da Microsoft o Configuração de carga de trabalho da Microsoft o Configuração de infraestrutura da Microsoft. ▪ Descoberta automática de: o Configuração de rede o Recursos de computação (servidores, clusters) o Recursos de armazenamento (LUNs, destinos iSCSi etc.) o Banco de dados (mecanismo, configuração, versão, compatibilidade) ▪ Análise de históricos de alterações no inventário (durante um período selecionado). ▪ Alocação de recursos, análise de utilização de capacidade. ▪ Análise de custos e alertas contínuos (utilização de recursos e licenciamento).	

	▪ Capacidade de recomendar provisionamento reduzido baseado nos padrões de utilização e carga de trabalho ▪ Análise e alerta contínuos de performance. ▪ Tarefas operacionais comuns de automação específica da carga de trabalho da Microsoft, como: o Backup e restauração o Aplicação de correções o Gerenciamento de estado da carga de trabalho o Gerenciamento de configuração ▪ Comparar performance necessária/média de soluções/aplicativos no local. ▪ Fornecer a instância, a correspondência de recursos e as recomendações na AWS com base nos testes comparativos. ▪ Realizar a POC e testes comparativos em soluções/aplicativos na AWS. ▪ Fornecer uma estimativa de TCO e utilização de recursos com base nos testes comparativos. ▪ Relatórios: o Relatório de performance, entrega e alerta (para relatórios). o Relatório de infraestrutura, entrega e alerta (para relatórios). o Configuração de carga de trabalho e relatório de integridade, entrega e alerta (para relatórios). o Aplicação de correções em relatório de performance, entrega e alerta (no caso de relatórios).	

Dados, análises e Machine Learning

Recursos obrigatórios da solução		**Cumprido S/N**
Integração e preparação de dados	A solução técnica deve poder: ▪ Consumo de dados de carga de trabalho e proposta de ação ▪ Anotar dados descritivos, estruturais, administrativos, de referência e estatísticos: o Banco de árvores sintáticas e de dependência, incluindo a identificação de correferência o Anotação semântica de texto, incluindo identificação de entidade nomeada para pesquisa, análise de sentimento e aplicativos de mineração de dados o Identificação de dados demográficos de idiomas, dialetos e falantes o Vídeo, imagem, arquivo de palavras, pdf etc. o Departamento, unidade de negócios, processo o Nível de proteção de segurança (Confidencial, Público, Privado etc.) o Tipo de objeto (prédio, pessoa, animal etc.) ▪ Mover e consolidar dados de fontes diferentes. ▪ Transformar e preparar dados para uma análise. ▪ Verificação de qualidade dos dados. ▪ Replicação de dados. ▪ Definição de perfil dos dados. ▪ Mecanismo de recursos – criação de novos recursos de entrada com base nos existentes.	

Soluções de plataforma	A solução técnica deve consistir em: ▪ Ferramentas fortemente integradas projetadas para trabalhar juntas e resolver desafios analíticos dentro de uma estrutura (de trabalho) padronizada, cujos componentes podem incluir: o Armazenamento o Processamento o Programação o Segurança o Instalações analíticas ▪ Capacitação de cientistas de dados e profissionais de machine learning com ferramentas para obter seus dados, treinar modelos preditivos e fazer previsões sobre novos dados.	
Soluções de SaaS e API	Esta categoria inclui soluções que habilitam recursos preditivos (IA/ML) em aplicativos de clientes: ▪ Web ▪ Cliente ▪ Estruturas (de trabalho)	
Business Intelligence e visualização	Soluções técnicas que transformam dados brutos em informações de negócios acionáveis usando tecnologias de processamento analítico, como: ▪ Relatórios ▪ Dashboarding ▪ Visualização de dados	
Governança de dados e segurança	Soluções técnicas para descobrir, categorizar e controlar dados. Isso inclui: ▪ Definição e aplicação de políticas. ▪ Segurança e gerenciamento de informações pessoais. ▪ Criação de catálogos de dados e glossários. ▪ Linhagem de dados. ▪ Mascaramento de dados.	

Requisitos técnicos da AWS

A seguir estão os requisitos técnicos para cada um dos 4 estudos de caso enviados pelo parceiro do APN. Cada um deve demonstrar que as soluções implantadas do parceiro do APN atendem às melhores práticas da AWS e aderem ao AWS Well-Architected Framework.

	Aplica-se a:				**Cumprido S/N**
	SaaS com vários locatários	SaaS com um único locatário	Implantação pelo cliente no local	Implantação pelo cliente na AWS	

Documentação exigida A documentação a seguir deve ser enviada como parte da Autoavaliação de competência.						
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 do APN 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 (Amazon VPC), as zonas de disponibilidade, as sub-redes e as conexões fora do sistema da AWS. ▪ Inclui elementos implantados fora da AWS, por exemplo, componentes locais ou dispositivos de hardware.	Sim. Um para a olução inteira e outro para cada Estudo de caso	Sim. Um para a olução inteira e outro para cada Estudo de caso	Sim. Um 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 do APN na AWS e inclui todas as seções descritas em "Requisitos de referência para guias de implantação"	Não	Não	Não	Sim. Um para a solução.	
Lista de verificação de validação preenchida	Para cada um dos quatro estudos de caso, 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	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, leia Criação de seu primeiro usuário administrador e grupo do IAM.	Sim	Sim	Não	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	Sim	Não	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 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.	Sim	Sim	Não	Não	
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	Sim	Não	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 enhas 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	Sim	Sim (para credenciais usadas para integração com a WS)	Sim (para credenciais usadas para integração com a WS)	
1.7 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	Sim	Sim (para credenciais usadas para integração com a WS)	Sim (para credenciais usadas para integração com a WS)	
1.8 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 AM receba um conjunto único de credenciais de egurança. Você também pode conceder permissões diferentes para cada usuário do IAM. Se necessário, você pode alterar ou revogar as ermissões do usuário do IAM	Sim	Sim	Não	Não	

	a qualquer momento. (Se você distribuir as credenciais do usuário raiz, será difícil revogá-las e impossível restringir suas permissões.)					
1.9 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 arefa específica, quais ações são permitidas por um determinado serviço e que permissões são necessárias para executar essas ações.	Sim	Sim	Sim (para soluções executadas fora da AWS e ntegradas por meio de unções do IAM, o cesso com o menor privilégio possível deve ser aplicado)	Sim (para soluções executadas fora da AWS e integradas por meio de funções do IAM, o cesso com o menor privilégio possível deve ser aplicado)	
1.10 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 cesso 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 eve fazer o mesmo.	Sim	Sim	Sim (credenciais usadas para integração com a AWS devem ser facilmente alteradas e ão devem ser definidas no ódigo)	Sim (credenciais usadas para integração com a AWS devem ser facilmente alteradas e ão devem ser definidas no ódigo)	
1.11 Todas as redenciais ociosas são criptografadas	O requisito é garantir a criptografia de todas as credenciais ociosas.	Sim	Sim	Sim (credenciais armazenadas na solução do arceiro usadas para integração com a AWS devem ser criptografadas)	Sim (credenciais armazenadas na solução do arceiro usadas para integração com a AWS devem ser criptografadas)	
1.12 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 Elastic Compute Cloud (Amazon EC2), uma função de tarefa do 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	Não	Não	
1.13 O AWS CloudTrail está habilitado para todas as contas da	O AWS CloudTrail deve estar habilitado em todas s contas da AWS e em todas as regiões. A isibilidade da atividade da conta da AWS é um specto essencial das melhores práticas de segurança e operações. Você	Sim	Sim	Não	Não	

AWS em cada região	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 esponder à atividade da conta da AWS.					
1.14 Logs do AWS CloudTrail são armazenados em um bucket do Amazon 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	Sim	Não	Não	
1.15 Versionamento ou exclusão com MFA deve estar habilitado no bucket do Amazon S3 que armazena os logs do AWS CloudTrail	O conteúdo do bucket de logs do AWS CloudTrail deve estar protegido por versionamento ou exclusão com MFA.	Sim	Sim	Não	Não	
1.16 Escopo de rupos de segurança do Amazon EC2 é eduzido	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	Não	Sim	
1.17 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 ada 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	Não	Não (a menos que a solução do parceiro executada na AWS exija o serviços S3)	
1.18 Buckets do Amazon S3 não foram configurados indevidamente para permitir acesso público.	Você deve garantir que todos os buckets que não evem permitir acesso público sejam configurados adequadamente para evitar o acesso público. Por padrão, todos os buckets do mazon S3 são privados e somente podem ser cessados 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 ocê 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	Não	Não (a menos que a solução do parceiro executada na AWS exija o serviços S3)	
1.19 Mecanismo de monitoramento implementado para detectar quando buckets ou objetos do	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 Trusted Advisor verifica os buckets do Amazon S3 que têm permissões de acesso aberto. As permissões de bucket que concedem acesso de istagem a todos podem resultar em custos superiores aos esperados se os objetos do bucket	Sim	Sim	Sim	Não (a menos que a solução do parceiro executada na AWS exija o serviços S3)	

Amazon S3 se tornam públicos	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 erificação do AWS Trusted Advisor examina as ermissões de bucket explícitas e as políticas de ucket associadas que podem substituir as permissões de bucket.					
1.20 Mecanismo de monitoramento implementado para detectar alterações em instâncias e contêineres do Amazon EC2	Todas as alterações efetuadas em instâncias ou contêineres do Amazon EC2 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 EC2 usados na solução. 2. Armazenar os dados que registram essas alterações em um local resiliente, externo à instância e ao contêiner do Amazon EC2. Entre os exemplos de mecanismos adequados, estão: a. Implantação de verificação de integridade de arquivos por meio de gerenciamento de configuração programado (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 EC2 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 EC2.	Sim	Sim	Não	Não	
1.21 Todos os dados são classificados	Todos os dados do cliente processados e rmazenados 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	Não	Não	
1.22 Todos os dados confidenciais são criptografados	Todos os dados do cliente classificados como onfidenciais são criptografados quando ociosos e em trânsito.	Sim	Sim	Não	Não	
1.23 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 KMS ou uma solução de parceiro do APN como o HashiCorp Vault.	Sim	Sim	Sim	Sim	
1.24 Todos os dados em trânsito são criptografados	Todos os dados em trânsito que atravessam um limite de VPC são criptografados.	Sim	Sim	Sim	Sim	

1.25 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 rocesso de resposta a incidentes. Por exemplo, a ealização de um exercício com simulações de segurança. Um ensaio deve ter sido realizado nos ltimos 12 meses para confirmar que: a. as pessoas apropriadas têm acesso ao ambiente. b. as erramentas adequadas estão disponíveis. c. as essoas apropriadas sabem o que fazer para responder aos diversos incidentes de segurança descritos no plano.	Sim	Sim	Não	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 liente nem sempre implemente esse recurso.	Sim	Sim	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 requência.	Sim	Sim	Não	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	Sim	Não	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	Sim	Não	Não	
2.5 Provisionamento e gerenciamento automatizados de infraestrutura	A solução deve usar uma ferramenta automatizada como o CloudFormation ou o erraform 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	Não	Não	
2.6 Backups de dados regulares são executados	Você deve executar backups regulares para um erviços de armazenamento resiliente. Os ackups asseguram a sua capacidade de ecuperação em cenários de erros administrativos, lógicos ou físicos. O Amazon S3 e o Amazon Glacier são serviços preferenciais para backup e arquivamento. Ambos são plataformas de armazenamento resilientes e de aixo custo. Ambos oferecem capacidade	Sim	Sim	Não	Não	

	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.					
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	Sim	Não	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	Não	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	Sim	Não	Sim	
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	Não	Não	
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	Sim	Não	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	Sim	Não	Não	
2.13 Plano de recuperação de desastres (DR) inclui a recuperação para outra conta da AWS	O plano de recuperação de desastres deve incluir uma estratégia de recuperação para outra conta 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 conta 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 conta da AWS.	Sim	Sim	Não	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 de SSH ou RDP não devem ser usadas para implantar atualizações na infraestrutura da AWS.	Sim	Sim	Não	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	Sim	Não	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	Sim	Não	Não	