Manual do usuário

# AWS Control Tower

# AWS Control Tower: Manual do usuário

# Table of Contents

# O que é o AWS Control Tower?

O AWS Control Tower oferece uma maneira simples de configurar e governar um ambiente com AWS várias contas, seguindo as melhores práticas prescritivas. O AWS Control Tower orquestra as capacidades de vários outros AWS serviços, incluindo AWS Organizations, AWS Service Catalog, e AWS IAM Identity Center, para construir uma landing zone em menos de uma hora. Os recursos são configurados e gerenciados em seu nome.

A orquestração do AWS Control Tower amplia os recursos do. AWS OrganizationsPara ajudar a evitar que suas organizações e contas se afastem, o que é uma divergência das melhores práticas, o AWS Control Tower aplica controles (às vezes chamados de grades de proteção). Por exemplo, você pode usar controles para ajudar a garantir que os registros de segurança e as permissões de acesso entre contas necessárias sejam criados, e não alterados.

Se você estiver hospedando mais do que um punhado de contas, é vantajoso ter uma camada de orquestração que facilite a implantação e a governança da conta. Você pode adotar o AWS Control Tower como sua principal forma de provisionar contas e infraestrutura. Com o AWS Control Tower, você pode aderir mais facilmente aos padrões corporativos, atender aos requisitos regulatórios e seguir as melhores práticas.

O AWS Control Tower permite que os usuários finais de suas equipes distribuídas provisionem novas AWS contas rapidamente, por meio de modelos de conta configuráveis no Account Factory. Enquanto isso, seus administradores centrais de nuvem podem monitorar se todas as contas estão alinhadas às políticas de conformidade estabelecidas em toda a empresa.

Resumindo, o AWS Control Tower oferece a maneira mais fácil de configurar e governar um AWS ambiente seguro, compatível e com várias contas, com base nas melhores práticas estabelecidas pelo trabalho com milhares de empresas. Para obter mais informações sobre como trabalhar com o AWS Control Tower e as melhores práticas descritas na estratégia de AWS várias contas, consulte. AWS estratégia de várias contas: orientação sobre as melhores práticas

## Recursos

O AWS Control Tower tem os seguintes recursos:

- Zona de pouso — Uma zona de pouso é um ambiente bem arquitetado, com várias contas, baseado nas melhores práticas de segurança e conformidade. É o contêiner corporativo que

contém todas as suas unidades organizacionais (OUs), contas, usuários e outros recursos que você deseja que estejam sujeitos à regulamentação de conformidade. Uma zona de destino pode ser dimensionada para atender às necessidades de uma empresa de qualquer tamanho.

- Controles — Um controle (às vezes chamado de guardrail) é uma regra de alto nível que fornece governança contínua para seu ambiente geral. AWS Ele é expressado em linguagem simples. Existem três tipos de controles: preventivos, detectivos e proativos. Três categorias de orientação se aplicam aos controles: obrigatórios, altamente recomendados ou eletivos. Para obter mais informações sobre controles, consulte Como os controles funcionam.
- Account Factory — An Account Factory é um modelo de conta configurável que ajuda a padronizar o provisionamento de novas contas com configurações de conta pré-aprovadas. O AWS Control Tower oferece um Account Factory integrado que ajuda a automatizar o fluxo de trabalho de provisionamento de contas na sua organização. Para ter mais informações, consulte Provisione e gerencie contas com o Account Factory.
- Painel — O painel oferece supervisão contínua de sua landing zone para sua equipe de administradores centrais de nuvem. Use o painel para ver contas provisionadas em toda a sua empresa, controles habilitados para aplicação de políticas, controles habilitados para detecção contínua de não conformidade com políticas e recursos não compatíveis organizados por contas e OUs.

# Como o AWS Control Tower interage com outros serviços AWS

O AWS Control Tower foi construído com base em AWS serviços confiáveis e confiáveis AWS Service Catalog AWS IAM Identity Center, incluindo, AWS Organizations e. Para ter mais informações, consulte Serviços integrados.

Você pode incorporar o AWS Control Tower a outros AWS serviços em uma solução que ajuda você a migrar suas cargas de trabalho existentes para o. AWS Para obter mais informações, consulte Como aproveitar as vantagens do AWS Control Tower e CloudEndure migrar cargas de trabalho para o. AWS

Configuração, governança e extensibilidade

- Configuração automatizada da conta: o AWS Control Tower automatiza a implantação e o registro de contas por meio de uma Account Factory (ou “máquina de venda automática”), que é criada como uma abstração sobre os produtos provisionados em. AWS Service Catalog O Account Factory pode criar e registrar AWS contas e automatiza o processo de aplicação de controles e políticas a essas contas.

- Governança centralizada: ao empregar os recursos do AWS Organizations, o AWS Control Tower configura uma estrutura que garante conformidade e governança consistentes em todo o seu ambiente de várias contas. O AWS Organizations serviço fornece recursos essenciais para gerenciar um ambiente de várias contas, incluindo governança central e gerenciamento de contas, criação de contas a partir de AWS Organizations APIs e políticas de controle de serviços (SCPs).

- Extensibilidade: você pode criar ou ampliar seu próprio ambiente do AWS Control Tower trabalhando diretamente no AWS Organizations console do AWS Control Tower e nele. Você pode ver suas alterações refletidas no AWS Control Tower depois de registrar suas organizações existentes e inscrever suas contas existentes no AWS Control Tower. Você pode atualizar sua zona de pouso do AWS Control Tower para refletir suas alterações. Se suas cargas de trabalho exigirem mais recursos avançados, você pode aproveitar outras soluções de AWS parceiros junto com o AWS Control Tower.

## Você é um usuário iniciante do AWS Control Tower?

Se você for um usuário iniciante desse serviço, será recomendável ler o seguinte:

1. Se você precisar de mais informações sobre como planejar e organizar sua landing zone, consulte Planeje sua zona de pouso da AWS Control Tower AWS estratégia de várias contas para sua zona de pouso da AWS Control Tower e.
2. Se você estiver pronto para criar a primeira zona de destino, consulte Comece a usar o AWS Control Tower.
3. Para obter informações sobre detecção e prevenção de oscilações, consulte Detecte e resolva desvios na AWS Control Tower.
4. Para obter detalhes de segurança, consulte Segurança na AWS Control Tower.
5. Para obter informações sobre como atualizar sua landing zone e contas de membros, consulteGerenciamento de atualizações de configuração no AWS Control Tower.

## Como o AWS Control Tower funciona

Esta seção descreve em alto nível como o AWS Control Tower funciona. Sua landing zone é um ambiente multicontas bem arquitetado para todos os seus recursos. AWS Você pode usar esse ambiente para impor normas de conformidade em todas as suas AWS contas.

# Estrutura de uma zona de pouso do AWS Control Tower

A estrutura de um landing zone no AWS Control Tower é a seguinte:

- Root — O pai que contém todas as outras OUs em sua landing zone.
- OU de segurança — Essa OU contém as contas de arquivamento de registros e auditoria. Essas contas geralmente são chamadas de contas compartilhadas. Ao iniciar sua landing zone, você pode escolher nomes personalizados para essas contas compartilhadas e tem a opção de trazer AWS contas existentes para o AWS Control Tower para fins de segurança e registro. No entanto, elas não podem ser renomeadas posteriormente e as contas existentes não podem ser adicionadas para fins de segurança e registro após o lançamento inicial.
- Sandbox OU — A OU Sandbox é criada quando você inicia sua landing zone, se você a habilitar. Essa e outras OUs registradas contêm as contas inscritas com as quais seus usuários trabalham para realizar suas cargas de trabalho da AWS.
- Diretório do IAM Identity Center — Esse diretório abriga os usuários do IAM Identity Center. Ele define o escopo das permissões para cada usuário do IAM Identity Center.
- Usuários do IAM Identity Center — Essas são as identidades que seus usuários podem assumir para realizar suas AWS cargas de trabalho em sua landing zone.

# O que acontece quando você configura uma landing zone

Quando você configura uma landing zone, o AWS Control Tower executa as seguintes ações em sua conta de gerenciamento em seu nome:

- Cria duas unidades AWS Organizations organizacionais (OUs): Segurança e Sandbox (opcional), contidas na estrutura raiz organizacional.
- Cria ou adiciona duas contas compartilhadas na OU de segurança: a conta Log Archive e a conta Audit.
- Cria um diretório nativo da nuvem no IAM Identity Center, com grupos pré-configurados e acesso de login único, se você escolher a configuração padrão do AWS Control Tower, ou se permitir que você autogerencie seu provedor de identidade.
- Aplica todos os controles obrigatórios e preventivos para aplicar as políticas.
- Aplica todos os controles de detetive obrigatórios para detectar violações de configuração.
- Os controles preventivos não são aplicados à conta de gerenciamento.

- Com exceção da conta de gerenciamento, os controles são aplicados à organização como um todo.

Gerenciamento seguro de recursos em sua zona de aterrissagem e contas do AWS Control Tower

- Quando você cria sua landing zone, vários AWS recursos são criados. Para usar o AWS Control Tower, você não deve modificar ou excluir esses recursos gerenciados do AWS Control Tower fora dos métodos suportados descritos neste guia. Excluir ou modificar esses recursos fará com que sua landing zone entre em um estado desconhecido. Para obter detalhes, consulte Orientação para criar e modificar recursos da AWS Control Tower
- Quando você ativa controles opcionais (aqueles com orientação altamente recomendada ou eletiva), o AWS Control Tower cria AWS recursos que são gerenciados em suas contas. Não modifique nem exclua recursos criados pelo AWS Control Tower. Isso pode fazer com que os controles entrem em um estado desconhecido.

## Quais são as contas compartilhadas?

No AWS Control Tower, as contas compartilhadas em sua landing zone são provisionadas durante a configuração: a conta de gerenciamento, a conta de arquivamento de registros e a conta de auditoria.

### O que é a conta de gerenciamento?

Essa é a conta que você criou especificamente para sua landing zone. Essa conta é usada para cobrar tudo em sua landing zone. Também é usado para o provisionamento de contas do Account Factory, bem como para gerenciar OUs e controles.

> **Note**
>
> Não é recomendável executar nenhum tipo de carga de trabalho de produção a partir de uma conta de gerenciamento do AWS Control Tower. Crie uma conta separada do AWS Control Tower para executar suas cargas de trabalho.

Para ter mais informações, consulte Conta de gerenciamento.

### O que é a conta de arquivamento de registros?

Essa conta funciona como um repositório para registros de atividades de API e configurações de recursos de todas as contas na landing zone.

Para ter mais informações, consulte Conta de arquivamento de logs.

### O que é a conta de auditoria?

A conta de auditoria é uma conta restrita projetada para dar às suas equipes de segurança e conformidade acesso de leitura e gravação a todas as contas em sua landing zone. Na conta de auditoria, você tem acesso programático às contas de revisão, por meio de uma função que é concedida somente às funções do Lambda. A conta de auditoria não permite que você faça login em outras contas manualmente. Para obter mais informações sobre funções e funções do Lambda, consulte Configurar uma função do Lambda para assumir uma função de outra. Conta da AWS

Para ter mais informações, consulte Conta de auditoria.

## Como os controles funcionam

Um controle é uma regra de alto nível que fornece governança contínua para seu AWS ambiente geral. Cada controle impõe uma única regra e ela é expressa em linguagem simples. Você pode alterar os controles eletivos ou altamente recomendados que estão em vigor, a qualquer momento, no console do AWS Control Tower ou nas APIs do AWS Control Tower. Os controles obrigatórios são sempre aplicados e não podem ser alterados.

Os controles preventivos evitam que ações ocorram. Por exemplo, o controle eletivo chamado Disallow Changes to Bucket Policy for Amazon S3 Buckets (anteriormente chamado de Disallow Policy Changes to Log Archive) impede qualquer alteração na política do IAM na conta compartilhada do arquivamento de logs. Qualquer tentativa de realizar uma ação evitada é negada e registrada. CloudTrail O recurso também está logado AWS Config.

Os controles de detetive detectam eventos específicos quando eles ocorrem e registram a ação. CloudTrail Por exemplo, o controle altamente recomendado chamado Detectar se a criptografia está habilitada para volumes do Amazon EBS anexados às instâncias do Amazon EC2 detecta se um volume não criptografado do Amazon EBS está conectado a uma instância do EC2 em sua landing zone.

Os controles proativos verificam se os recursos estão em conformidade com as políticas e os objetivos da sua empresa, antes que os recursos sejam provisionados em suas contas. Se os

recursos estiverem fora de conformidade, eles não serão provisionados. Os controles proativos monitoram os recursos que seriam implantados em suas contas por meio de AWS CloudFormation modelos.

Para aqueles que estão familiarizados com AWS: No AWS Control Tower, os controles preventivos são implementados com políticas de controle de serviços (SCPs). Os controles de detetive são implementados com AWS Config regras. Os controles proativos são implementados com AWS CloudFormation ganchos.

### Related Topics

- Detecte e resolva desvios na AWS Control Tower

## Como o AWS Control Tower funciona com StackSets

O AWS Control Tower usa AWS CloudFormation StackSets para configurar recursos em suas contas. Cada conjunto de pilhas tem StackInstances o que corresponde às contas e a Regiões da AWS cada conta. O AWS Control Tower implanta uma instância de conjunto de pilhas por conta e região.

O AWS Control Tower aplica atualizações a determinadas contas de Regiões da AWS forma seletiva, com base em AWS CloudFormation parâmetros. Quando as atualizações são aplicadas a algumas instâncias de pilha, outras instâncias de pilha podem ser deixadas no status Outdated (Desatualizada). Esse comportamento é esperado e normal.

Quando uma instância de pilha entra no status Outdated (Desatualizada), isso geralmente significa que a pilha correspondente a essa instância de pilha não está alinhada ao modelo mais recente no conjunto de pilhas. A pilha permanece no modelo mais antigo, portanto, pode não incluir os recursos ou parâmetros mais recentes. A pilha ainda é completamente utilizável.

Aqui está um resumo rápido do comportamento esperado, com base nos AWS CloudFormation parâmetros especificados durante uma atualização:

Se a atualização do conjunto de pilhas incluir alterações no modelo (ou seja, se as `TemplateURL` propriedades `TemplateBody` ou forem especificadas) ou se a `Parameters` propriedade for especificada, AWS CloudFormation marcará todas as instâncias da pilha com o status Desatualizado antes de atualizar as instâncias da pilha nas contas especificadas e. Regiões da AWS Se a atualização do conjunto de pilhas não incluir alterações no modelo ou nos parâmetros, AWS

CloudFormation atualize as instâncias da pilha nas contas e regiões especificadas, deixando todas as outras instâncias da pilha com o status atual de instância da pilha. Para atualizar todas as instâncias de pilha associadas a um conjunto de pilhas, não especifique as propriedades `Accounts` ou `Regions`.

Para obter mais informações, consulte Atualizar seu conjunto de pilhas no Guia do AWS CloudFormation usuário.

# Terminologia

Aqui está uma rápida revisão de alguns termos que você verá na documentação da AWS Control Tower.

Primeiro, é bom saber que o AWS Control Tower compartilha muita terminologia com o AWS Organizations serviço, incluindo os termos organização e unidade organizacional (OU), que aparecem em todo este documento.

- Para obter mais informações sobre organizações eOUs, consulte AWS Organizations terminologia e conceitos. Se você é novato na AWS Control Tower, essa terminologia é um bom lugar para começar.
- AWS Organizationsé um AWS serviço que ajuda você a governar centralmente seu ambiente à medida que você cresce e expande suas cargas de trabalho. AWS AWSA Control Tower depende AWS Organizations da criação de contas, da aplicação de controles preventivos no nível da UO e do fornecimento de faturamento centralizado.
- Uma AWS conta Account Factory é uma AWS conta provisionada usando Account Factory na AWS Control Tower. Às vezes, o Account Factory é chamado informalmente de “máquina de venda automática” para contas.
- Sua região de origem da AWS Control Tower é a AWS região na qual sua zona de pouso da AWS Control Tower foi implantada. Você pode ver sua região de origem nas configurações do seu landing zone.
- AWS Service Catalogpermite que você gerencie serviços de TI comumente implantados de forma centralizada. No contexto deste documento, o Account Factory usa AWS Service Catalog para provisionar novas AWS contas, incluindo contas de modelos personalizados.
- AWS CloudFormation StackSetssão um tipo de recurso que amplia a funcionalidade das pilhas para que você possa criar, atualizar ou excluir pilhas em várias contas e regiões com uma única operação e um único CloudFormation modelo.
- Uma instância de pilha é uma referência a uma pilha em uma conta de destino em uma região.
- Uma pilha é uma coleção de AWS recursos que você pode gerenciar como uma única unidade.
- Um agregador é um tipo de AWS Config recurso que coleta dados de AWS Config configuração e conformidade de várias contas e regiões da organização, permitindo que você visualize e consulte esses dados de conformidade em uma única conta.
- Um pacote de conformidade é um conjunto de AWS Config regras e ações de remediação que podem ser implantadas como uma única entidade em uma conta e uma região, ou em uma

organização em. AWS Organizations Você pode usar um pacote de conformidade para ajudar a personalizar seu ambiente da AWS Control Tower. Para blogs técnicos que fornecem mais detalhes, consulte Informações relacionadas.

- Uma linha de base no AWS Control Tower é um grupo de recursos e configurações específicas que você pode aplicar a um alvo. A meta básica mais comum pode ser uma unidade organizacional (OU). Por exemplo, a linha de base chamada `AWSControlTowerBaseline` está disponível para ajudar a registrá-lo no OUs AWS Control Tower. Durante a configuração e atualização da zona de pouso, a meta básica pode ser uma conta compartilhada ou uma configuração específica para a zona de pouso como um todo.
- Blueprint: Um blueprint é um artefato que encapsula alguns metadados, que descreve os componentes da infraestrutura que são implantados em uma conta. Por exemplo, um AWS CloudFormation modelo pode servir como um modelo para uma conta da AWS Control Tower.
- Drift: uma alteração em um recurso instalado e configurado pelo AWS Control Tower. Recursos sem desvio permitem que a AWS Control Tower funcione corretamente.
- Recurso não compatível: um recurso que viola uma AWS Config regra que define um controle específico de detetive.
- Conta compartilhada: uma das três contas que a AWS Control Tower cria automaticamente quando você configura sua landing zone: a conta de gerenciamento, a conta de arquivamento de registros e a conta de auditoria. Você pode escolher nomes personalizados para a conta de arquivamento de registros e a conta de auditoria durante a configuração.
- Conta de membro: uma conta de membro pertence à organização AWS Control Tower. A conta do membro pode ser cadastrada ou cancelada no Control TowerAWS. Quando uma OU registrada contém uma combinação de contas inscritas e não inscritas:
  - Os controles preventivos habilitados na OU se aplicam a todas as contas dentro dela, inclusive as não inscritas. Isso é verdade porque os controles preventivos são aplicados SCPs no nível da OU, não no nível da conta. Para obter mais informações, consulte Herança para políticas de controle de serviços na AWS Organizations documentação.
  - Os controles de detetive ativados na OU não se aplicam a contas não inscritas.

  Uma conta só pode ser membro de uma organização por vez, e suas cobranças são cobradas na conta de gerenciamento dessa organização. Uma conta de membro pode ser movida para o contêiner raiz de uma organização.
- AWS conta: uma AWS conta atua como um contêiner de recursos e um limite de isolamento de recursos. Uma AWS conta pode ser associada ao faturamento e ao pagamento. Uma AWS conta é diferente de uma conta de usuário (às vezes chamada de conta de IAM usuário) no AWS Control

Tower. As contas criadas por meio do processo de provisionamento do Account Factory são AWS contas. AWS contas também podem ser adicionadas à AWS Control Tower por meio do processo de inscrição da conta ou registro da OU.

- Controle: um controle (também conhecido como corrimão) é uma regra de alto nível que fornece governança contínua para seu ambiente geral da AWS Control Tower. Cada controle impõe uma única regra. Os controles preventivos são implementados comSCPs. Os controles de detetive são implementados com AWS Config regras. Os controles proativos são implementados com AWS CloudFormation ganchos. Para obter mais informações, consulte Como os controles funcionam.
- Zona de aterrissagem: uma landing zone é um ambiente em nuvem que oferece um ponto de partida recomendado, incluindo contas padrão, estrutura de contas, layouts de rede e segurança, etc. A partir de uma landing zone, você pode implantar cargas de trabalho que utilizam suas soluções e aplicativos.
- OU aninhada: uma OU aninhada na AWS Control Tower é uma OU contida em outra OU. Uma OU aninhada pode ter exatamente uma OU principal, e cada conta pode ser membro de exatamente uma OU. Aninhado, OUs crie uma hierarquia. Quando você anexa uma política a uma das da OUs hierarquia, ela flui para baixo e afeta todas as OUs contas abaixo dela. Uma hierarquia de OU aninhada na AWS Control Tower pode ter no máximo cinco níveis de profundidade.
- OU principal: A OU imediatamente acima da OU atual na hierarquia. Cada OU pode ter exatamente uma OU principal.
- OU secundária: Qualquer OU abaixo da OU atual na hierarquia. Uma OU pode ter muitos filhosOUs.
- Hierarquia da OU: na AWS Control Tower, a hierarquia de aninhada OUs pode ter até cinco níveis. A ordem de aninhamento é chamada de Níveis. O topo da hierarquia é designado como Nível 1.
- OU de nível superior: Uma OU de nível superior é qualquer OU que esteja diretamente sob a raiz, não a raiz em si. A raiz não é considerada uma OU.
- Governada: uma região governada é gerenciada e controlada em seu ambiente pela AWS Control Tower, de acordo com as políticas de governança definidas pela sua organização. Eles Regiões da AWS são monitorados de acordo com as melhores práticas e políticas organizacionais. Seus recursos nessas regiões são protegidos quando você ativa os controles da AWS Control Tower.
- Não governado: as regiões que mostram o status Não governado não são controladas nem monitoradas pela AWS Control Tower. Eles Regiões da AWS geralmente não seguem as mesmas políticas de governança que a AWS Control Tower impõe. Você pode criar recursos nessas regiões, mas esses recursos não são protegidos pelos controles da AWS Control Tower.

- Negado: uma região negada é bloqueada especificamente pela AWS Control Tower. Em seu ambiente AWS Control Tower, você não pode provisionar recursos neles Regiões da AWS.

# Definição de preço

Não há cobrança adicional pelo uso do AWS Control Tower. Você paga somente pelos AWS serviços habilitados pelo AWS Control Tower e pelos serviços que você usa na sua landing zone. Por exemplo, você paga pelo Service Catalog pelo provisionamento de contas com o Account Factory e AWS CloudTrail pelos eventos rastreados na sua landing zone. Para obter informações sobre os preços e as taxas associados à AWS Control Tower, consulte a definição de preço da AWS Control Tower.

Se você estiver executando cargas de trabalho efêmeras a partir de contas no AWS Control Tower, poderá observar um aumento nos custos associados a. AWS ConfigPara obter detalhes, consulte Definição de preço doAWS Config. Entre em contato com seu representante de AWS conta para obter informações mais específicas sobre como gerenciar esses custos. Para saber mais sobre como AWS Config funciona com o AWS Control Tower, consulteMonitore as mudanças de recursos com AWS Config.

Se você implementar AWS CloudTrail trilhas fora da AWS Control Tower, poderá usá-las com o AWS Control Tower. No entanto, você pode incorrer em cobranças duplicadas se também optar por trilhas gerenciadas pelo AWS Control Tower. Não recomendamos a configuração de trilhas externas, a menos que você tenha um requisito específico. Se você optar por participar durante a configuração ou atualização do landing zone, o AWS Control Tower configura e ativa uma CloudTrail trilha em nível organizacional para você na conta de gerenciamento. Para obter informações sobre o gerenciamento de CloudTrail custos, consulte Gerenciamento de CloudTrail custos.

# Configuração

Antes de usar AWS Control Tower pela primeira vez, siga as etapas nesta seção para criar um AWS conte e proteja sua AWS Control Tower conta de gerenciamento. Para obter informações sobre tarefas adicionais de configuração específicas para AWS Control Tower, consulte Comece a usar o AWS Control Tower.

## Inscreva-se para AWS

Quando você se inscreve no Amazon Web Services (AWS), seu AWS a conta é automaticamente inscrita para todos os serviços em AWS, incluindo AWS Control Tower. Se você tem um AWS já tem uma conta, vá para a próxima tarefa. Se você não tem um AWS conta, use o procedimento a seguir para criar uma.

Anote seu AWS número da conta, porque você precisa dele para outras tarefas.

### Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar uma.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário root tem acesso a todos Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

# Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilitar AWS IAM Identity Center e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Consolecomo proprietário da conta, escolhendo o usuário root e inserindo seu Conta da AWS endereço de e-mail. Na próxima página, insira sua senha.

   Para obter ajuda para fazer login usando o usuário root, consulte Como fazer login como usuário root no Início de Sessão da AWS Guia do usuário.
2. Ative a autenticação multifator (MFA) para seu usuário root.

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu Conta da AWS usuário root (console) no Guia do IAM usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

   Para obter instruções, consulte Habilitando AWS IAM Identity Center no AWS IAM Identity Center Guia do usuário.
2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como sua fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no AWS IAM Identity Center Guia do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no AWS portal de acesso no Início de Sessão da AWS Guia do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

   Para obter instruções, consulte Criar um conjunto de permissões no AWS IAM Identity Center Guia do usuário.
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no AWS IAM Identity Center Guia do usuário.

> **Segurança para suas contas**
>
> Você pode encontrar orientações adicionais sobre como configurar as melhores práticas que protejam a segurança de seu AWS Control Tower contas, no AWS Organizations documentação.
>
> - Melhores práticas para a conta de gerenciamento
> - Melhores práticas para contas de membros

# Próxima etapa

Comece a usar o AWS Control Tower

# Comece a usar o AWS Control Tower

Esse procedimento de introdução é destinado aos administradores do AWS Control Tower. Siga este procedimento quando estiver pronto para configurar sua landing zone usando o console ou as APIs do AWS Control Tower.

Se você é um AWS cliente atualmente, mas é novo no AWS Control Tower, talvez queira revisar a seção chamada Planeje sua zona de pouso da AWS Control Tower antes de continuar.

Tópicos



## Guia de início rápido do AWS Control Tower

Se você é novato AWS, pode seguir as etapas nesta seção para começar a usar rapidamente o AWS Control Tower. Se você preferir personalizar seu ambiente do AWS Control Tower imediatamente, consulte Etapa 2. Configure e lance sua landing zone .

> **Note**
>
> O AWS Control Tower configura serviços pagos AWS CloudTrail, como Amazon AWS ConfigCloudWatch, Amazon S3 e Amazon VPC. Quando usados, esses serviços podem incorrer em custos, conforme mostrado na página de preços. O console AWS de gerenciamento mostra o uso de quaisquer serviços pagos e os custos incorridos. Nenhum custo adicional é criado pelo próprio AWS Control Tower.

Antes de começar

A decisão mais importante a ser tomada antes de iniciar o processo de configuração é escolher sua região de origem. Sua região de origem é a AWS região na qual você executará a maioria das suas

cargas de trabalho ou armazenará a maioria dos seus dados. Ele não pode ser alterado depois de configurar sua zona de pouso do AWS Control Tower. Para obter mais informações sobre como escolher uma região de origem, consulte Dicas administrativas para configuração da landing zone .

> **Note**
>
> Por padrão, o AWS Control Tower escolhe a região na qual sua conta está operando atualmente como sua região de origem. Você pode ver sua região atual no canto superior direito da tela do console AWS de gerenciamento.

O procedimento de início rápido pressupõe que você aceitará os valores padrão para os recursos em seu ambiente do AWS Control Tower. Muitas dessas opções podem ser alteradas posteriormente. Algumas opções únicas estão listadas na seção chamadaExpectativas para a configuração da landing zone .

Se você criou uma nova AWS conta, ela atende automaticamente aos pré-requisitos necessários para configurar o AWS Control Tower. Você pode prosseguir com as etapas a seguir.

Etapas de início rápido

1. Entre no console de AWS gerenciamento com suas credenciais de usuário administrador.
2. Navegue até o console do AWS Control Tower em https://console.aws.amazon.com/controltower.
3. Verifique se você está trabalhando na região de origem desejada.
4. Escolha Configurar landing zone.
5. Siga as instruções no console, aceitando todos os valores padrão. Você precisará digitar o endereço de e-mail da sua conta, uma conta de arquivamento de registros e uma conta de auditoria.
6. Confirme suas escolhas e escolha Configurar landing zone.
7. O AWS Control Tower leva cerca de 30 minutos para configurar todos os recursos em sua landing zone.

Para obter uma versão mais detalhada de como configurar o AWS Control Tower, incluindo formas de personalizar seu ambiente, leia e siga os procedimentos nos próximos tópicos.

> **Note**
>
> Se você for um cliente pela primeira vez e encontrar um problema de configuração, entre em contato com o AWS Support para obter assistência no diagnóstico.

## Pré-requisito: verificações automáticas de pré-lançamento para sua conta de gerenciamento

Antes de configurar a landing zone, o AWS Control Tower executa automaticamente uma série de verificações de pré-lançamento em sua conta. Não é necessária nenhuma ação de sua parte para essas verificações, que garantem que sua conta de gerenciamento esteja pronta para as mudanças que estabelecem sua landing zone. Aqui estão as verificações que o AWS Control Tower executa antes de configurar uma landing zone:

- Os limites de serviço existentes para o Conta da AWS devem ser suficientes para o lançamento do AWS Control Tower. Para ter mais informações, consulte Limitações e cotas na AWS Control Tower.
- Eles Conta da AWS devem ser assinantes dos seguintes AWS serviços:
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (IAM)
  - AWS Lambda

> **Note**
>
> Por padrão, todas as contas são inscritas nesses serviços.

# Considerações para clientes AWS IAM Identity Center (IAM Identity Center)

- Se o AWS IAM Identity Center (IAM Identity Center) já estiver configurado, a região de origem do AWS Control Tower deve ser a mesma que a região do IAM Identity Center.
- O IAM Identity Center só pode ser instalado na conta de gerenciamento de uma organização.
- Três opções se aplicam ao seu diretório do IAM Identity Center, com base na fonte de identidade que você escolher:
  - Armazenamento de usuários do IAM Identity Center: se o AWS Control Tower estiver configurado com o IAM Identity Center, o AWS Control Tower cria grupos no diretório do IAM Identity Center e provisiona o acesso a esses grupos, para o usuário selecionado, para contas de membros.
  - Active Directory: se o IAM Identity Center for AWS Control Tower estiver configurado com o Active Directory, o AWS Control Tower não gerenciará o diretório do IAM Identity Center. Ele não atribui usuários ou grupos a novas AWS contas.
  - Provedor de identidade externo: se o IAM Identity Center for AWS Control Tower estiver configurado com um provedor de identidade externo (IdP), o AWS Control Tower criará grupos no diretório do IAM Identity Center e provisiona o acesso a esses grupos para o usuário selecionado para contas de membros. Você pode especificar um usuário existente do seu IdP externo no Account Factory durante a criação da conta, e o AWS Control Tower concede a esse usuário acesso à conta recém-vendida ao sincronizar usuários com o mesmo nome entre o IAM Identity Center e o IdP externo. Você também pode criar grupos em seu IdP externo para corresponder aos nomes dos grupos padrão no AWS Control Tower. Quando você atribui usuários a esses grupos, esses usuários terão acesso às suas contas inscritas.

  Para obter mais informações sobre como trabalhar com o IAM Identity Center e o AWS Control Tower, consulte Coisas que você deve saber sobre as contas do IAM Identity Center e o AWS Control Tower

## Considerações para AWS Config e para clientes AWS CloudTrail

- Conta da AWS Não é possível ter acesso confiável habilitado na conta de gerenciamento da organização para AWS Config ou CloudTrail. Para obter informações sobre como desabilitar o acesso confiável, consulte a AWS Organizations documentação sobre como habilitar ou desabilitar o acesso confiável.

- Se você tem um AWS Config gravador, canal de entrega ou configuração de agregação existente em qualquer conta existente que planeja inscrever no AWS Control Tower, você deve modificar ou remover essas configurações antes de começar a cadastrar as contas, depois que sua landing zone estiver configurada. Essa pré-verificação não se aplica à conta de gerenciamento do AWS Control Tower durante o lançamento da landing zone. Para ter mais informações, consulte Inscrever contas que tenham recursos existentes AWS Config.
- Se você estiver executando cargas de trabalho efêmeras a partir de contas no AWS Control Tower, poderá observar um aumento nos custos associados ao Config. AWS Entre em contato com seu representante de AWS conta para obter informações mais específicas sobre como gerenciar esses custos.
- Quando você inscreve uma conta no AWS Control Tower, sua conta é governada pela AWS CloudTrail trilha da organização da AWS Control Tower. Se você já tiver uma implantação de uma CloudTrail trilha na conta, poderá ver cobranças duplicadas, a menos que exclua a trilha existente da conta antes de inscrevê-la no AWS Control Tower. Para obter informações sobre trilhas em nível organizacional e o AWS Control Tower, consulte. Definição de preço

> **Note**
>
> Durante o lançamento, os endpoints do AWS Security Token Service (STS) devem ser ativados na conta de gerenciamento para todas as regiões governadas pelo AWS Control Tower. Caso contrário, a execução pode falhar no meio do processo de configuração.

# Comece a usar o AWS Control Tower no console

Esse procedimento de introdução é destinado aos administradores da AWS Control Tower. Siga este procedimento quando estiver pronto para configurar seu landing zone usando o console AWS Control Tower. Do início ao fim, deve levar cerca de meia hora. Esse procedimento requer alguns pré-requisitos e três etapas principais.

Se você é um AWS cliente atualmente, mas é novo no AWS Control Tower, talvez queira revisar a seção chamada Planeje sua zona de pouso da AWS Control Tower antes de continuar.

Tópicos

- Expectativas para a configuração da landing zone
- Etapa 1: Crie os endereços de e-mail da sua conta compartilhada

- Etapa 2. Configure e lance sua landing zone
- Etapa 3. Revise e configure a landing zone

## Expectativas para a configuração da landing zone

O processo de configuração da sua landing zone da AWS Control Tower tem várias etapas. Certos aspectos da sua zona de pouso do AWS Control Tower são configuráveis. Outras opções não podem ser alteradas após a configuração.

Itens principais a serem configurados durante a configuração

- Você pode selecionar seus nomes de OU de nível superior durante a configuração e também pode alterar os nomes de OU depois de configurar sua landing zone. Por padrão, os níveis superiores OUs são chamados de Segurança e Sandbox. Para obter mais informações, consulte Diretrizes para configurar um ambiente bem arquitetado.
- Durante a configuração, você pode selecionar nomes personalizados para as contas compartilhadas que a AWS Control Tower cria, chamadas de arquivamento de registros e auditoria por padrão, mas não pode alterar esses nomes após a configuração. (Essa é uma seleção única.)
- Durante a configuração, você pode, opcionalmente, especificar AWS contas existentes para o AWS Control Tower usar como contas de auditoria e arquivamento de registros. Se você planeja especificar AWS contas existentes e se essas contas têm AWS Config recursos existentes, você deve excluir os AWS Config recursos existentes antes de poder inscrever as contas na AWS Control Tower. (Essa é uma seleção única.)
- Se você estiver se configurando pela primeira vez ou se estiver atualizando para a versão 3.0 da landing zone, você pode escolher se deseja permitir que a AWS Control Tower configure uma AWS CloudTrail trilha em nível organizacional para sua organização ou pode optar por não usar trilhas gerenciadas pela Control Tower e gerenciar suas AWS próprias trilhas. CloudTrail Você pode ativar ou desativar as trilhas de nível organizacional gerenciadas pela AWS Control Tower sempre que atualizar sua landing zone.
- Opcionalmente, você pode definir uma política de retenção personalizada para seu bucket de log e bucket de acesso ao log do Amazon S3 ao configurar ou atualizar sua landing zone.
- Opcionalmente, você pode especificar um blueprint previamente definido para uso no provisionamento de contas de membros personalizadas no console do Control Tower. AWS Você pode personalizar contas posteriormente se não tiver um plano disponível. Consulte Personalize contas com Account Factory Customization (AFC).

Opções de configuração que não podem ser desfeitas

- Você não pode mudar sua região de origem depois de configurar sua landing zone.
- Se você estiver provisionando contas do Account Factory comVPCs, elas não VPC CIDRs poderão ser alteradas depois de criadas.

## Etapa 1: Crie os endereços de e-mail da sua conta compartilhada

Se você estiver configurando sua landing zone em uma nova Conta da AWS, consulteConfiguração.

- Para configurar sua landing zone com novas contas compartilhadas, o AWS Control Tower requer dois endereços de e-mail exclusivos que ainda não estejam associados a um Conta da AWS. Cada um desses endereços de e-mail servirá como uma caixa de entrada colaborativa — uma conta de e-mail compartilhada — destinada aos vários usuários da sua empresa que realizarão trabalhos específicos relacionados à AWS Control Tower.
- Se você estiver configurando a AWS Control Tower pela primeira vez e se estiver trazendo contas existentes de segurança e arquivamento de registros para a AWS Control Tower, poderá inserir os endereços de e-mail atuais das AWS contas existentes.

Os endereços de e-mail são necessários para:

- Conta de auditoria — Essa conta é para sua equipe de usuários que precisam acessar as informações de auditoria disponibilizadas pela AWS Control Tower. Você também pode usar essa conta como o ponto de acesso para ferramentas de terceiros que realizarão auditoria programática do ambiente para ajudar a auditar para fins de conformidade.
- Conta de arquivamento de registros — Essa conta é para sua equipe de usuários que precisam acessar todas as informações de registro de todas as suas contas inscritas registradas OUs em seu landing zone.

Essas contas são configuradas na OU de segurança quando você cria sua landing zone. Como prática recomendada, recomendamos que, ao realizar ações nessas contas, você use um usuário do IAM Identity Center com as permissões apropriadas.

> **Note**
>
> Se você especificar AWS contas existentes como contas de auditoria e arquivamento de registros, as contas existentes deverão passar por algumas verificações de pré-lançamento

para garantir que nenhum recurso esteja em conflito com os requisitos da AWS Control Tower. Se essas verificações não forem bem-sucedidas, a configuração da sua landing zone pode não ser bem-sucedida. Em particular, as contas não devem ter AWS Config recursos existentes. Para obter mais informações, consulte Considerações sobre como trazer contas de segurança ou registro existentes.

Para fins de clareza, este Guia do Usuário sempre se refere às contas compartilhadas por seus nomes padrão: arquivo de log e auditoria. Ao ler este documento, lembre-se de substituir os nomes personalizados que você atribuiu inicialmente a essas contas, caso opte por personalizá-las. Você pode ver suas contas com seus nomes personalizados na página de detalhes da conta.

**Note**

Estamos alterando nossa terminologia em relação aos nomes padrão de algumas unidades organizacionais da AWS Control Tower (OUs) para alinhar com a estratégia de AWS várias contas. Você pode notar algumas inconsistências enquanto estamos fazendo uma transição para melhorar a clareza desses nomes. A OU de segurança era anteriormente chamada de OU Core. A Sandbox OU era anteriormente chamada de OU personalizada.

## Etapa 2. Configure e lance sua landing zone

Antes de iniciar sua zona de pouso da AWS Control Tower, determine a região de origem mais apropriada. Para obter mais informações, consulte Dicas administrativas para configuração da landing zone .

**Important**

Mudar sua região de origem depois de implantar sua zona de pouso da AWS Control Tower requer descomissionamento, bem como a assistência do Support. AWS Essa prática não é recomendada.

Aprenda a configurar e lançar sua landing zone usando o AWS CLI inComece a usar o AWS Control Tower usando APIs.

Para configurar e iniciar sua landing zone no console, execute a seguinte série de etapas.

Prepare-se: navegue até o console da AWS Control Tower

1. Abra um navegador da Web e navegue até o console da AWS Control Tower em https://console.aws.amazon.com/controltower.
2. No console, verifique se você está trabalhando na região de origem desejada para o AWS Control Tower. Em seguida, escolha Configurar sua landing zone.

## Etapa 2a. Revise e selecione suas AWS regiões

Certifique-se de ter designado corretamente a AWS região que você selecionou para sua região de origem. Depois de implantar a AWS Control Tower, você não poderá alterar a região de origem.

Nesta seção do processo de configuração, você pode adicionar quaisquer AWS regiões adicionais de que precisar. Você pode adicionar mais regiões posteriormente, se necessário, e remover regiões da governança.

Para selecionar AWS regiões adicionais para governar

1. O painel mostra as seleções de região atuais. Abra o menu suspenso para ver uma lista de regiões adicionais disponíveis para governança.
2. Marque a caixa ao lado de cada região para incluir a governança da AWS Control Tower. Sua seleção de região de origem não é editável.

Para negar acesso a determinadas regiões

Para negar acesso a AWS recursos e cargas de trabalho em determinadas AWS regiões, selecione Ativado na seção do controle de negação de região. Por padrão, a configuração desse controle é Não ativada.

## Etapa 2b. Configure suas unidades organizacionais (OUs)

Se você aceitar os nomes padrão dessesOUs, não será necessário realizar nenhuma ação para que a configuração continue. Para alterar os nomes doOUs, insira os novos nomes diretamente no campo do formulário.

- OU básica — A AWS Control Tower depende de uma OU básica que é inicialmente chamada de OU de segurança. Você pode alterar o nome dessa OU durante a configuração inicial e depois, na página de detalhes da OU. Essa OU de segurança contém suas duas contas compartilhadas, que por padrão são chamadas de conta de arquivamento de log e conta de auditoria.

- OU adicional — A AWS Control Tower pode configurar um ou mais adicionais OUs para você. Recomendamos que você provisione pelo menos uma OU adicional em sua landing zone, além da OU de segurança. Se essa OU adicional for destinada a projetos de desenvolvimento, recomendamos que você a nomeie como Sandbox OU, conforme indicado noDiretrizes para configurar um ambiente bem arquitetado. Se você já tiver uma OU existente AWS Organizations, talvez veja a opção de pular a configuração de uma OU adicional no AWS Control Tower.

## Etapa 2c. Configure suas contas compartilhadas, registro e criptografia

Nesta seção do processo de configuração, o painel mostra as seleções padrão para os nomes das suas contas compartilhadas da AWS Control Tower. Essas contas são uma parte essencial da sua landing zone. Não mova nem exclua essas contas compartilhadas. Você pode escolher nomes personalizados para as contas de auditoria e arquivamento de registros durante a configuração. Como alternativa, você tem uma opção única para especificar AWS contas existentes como suas contas compartilhadas.

Você deve fornecer endereços de e-mail exclusivos para seu arquivo de registros e contas de auditoria e pode verificar o endereço de e-mail fornecido anteriormente para sua conta de gerenciamento. Escolha o botão Editar para alterar os valores padrão editáveis.

Sobre as contas compartilhadas

- A conta de gerenciamento — A conta de gerenciamento da AWS Control Tower faz parte do nível raiz. A conta de gerenciamento permite o faturamento da AWS Control Tower. A conta também tem permissões de administrador para sua landing zone. Você não pode criar contas separadas para cobrança e permissões de administrador na AWS Control Tower.

  O endereço de e-mail mostrado para a conta de gerenciamento não é editável durante essa fase de configuração. Ela é exibida como uma confirmação, para que você possa verificar se está editando a conta de gerenciamento correta, caso tenha várias contas.
- As duas contas compartilhadas — Você pode escolher nomes personalizados para essas duas contas ou trazer suas próprias contas e fornecer um endereço de e-mail exclusivo para cada conta, nova ou existente. Se você optar por fazer com que a AWS Control Tower crie novas contas compartilhadas para você, os endereços de e-mail ainda não devem ter AWS contas associadas.

Para configurar as contas compartilhadas, preencha as informações solicitadas.

1. No console, insira um nome para a conta inicialmente chamada de conta de arquivamento de registros. Muitos clientes decidem manter o nome padrão dessa conta.
2. Forneça um endereço de e-mail exclusivo para essa conta.
3. Insira um nome para a conta inicialmente chamada de conta de auditoria. Muitos clientes optam por chamá-la de conta de segurança.
4. Forneça um endereço de e-mail exclusivo para essa conta.

Opcionalmente, configure a retenção de registros

Durante essa fase de configuração, você pode personalizar a política de retenção de registros para buckets do Amazon S3 que armazenam seus AWS CloudTrail registros na AWS Control Tower, em incrementos de dias ou anos, até um máximo de 15 anos. Se você optar por não personalizar sua retenção de registros, as configurações padrão são de um ano para registro de conta padrão e 10 anos para registro de acesso. Esse recurso também está disponível quando você atualiza ou redefine sua landing zone.

Opcionalmente, Conta da AWS autogerencie o acesso

Você pode selecionar se o AWS Control Tower configura o Conta da AWS acesso com AWS Identity and Access Management (IAM) ou se deseja autogerenciar o Conta da AWS acesso — seja com usuários, funções e permissões do AWS IAM Identity Center que você pode configurar e personalizar sozinho, ou com outro método, como um IdP externo, seja para federação direta de contas ou federação de várias contas por meio do Identity Center. IAM Você pode alterar essa seleção posteriormente.

Por padrão, o AWS Control Tower configura o AWS IAM Identity Center para sua landing zone, de acordo com as diretrizes de melhores práticas definidas em Organizando seu AWS ambiente usando várias contas. A maioria dos clientes escolhe o padrão. Às vezes, métodos alternativos de acesso são necessários para conformidade regulatória em setores ou países específicos ou Regiões da AWS onde o AWS IAM Identity Center não está disponível.

A seleção de provedores de identidade no nível da conta não é suportada. Essa opção se aplica somente à landing zone como um todo.

Para obter mais informações, consulte IAMOrientação do Identity Center.

### Opcionalmente, configure trilhas AWS CloudTrail

Como prática recomendada, recomendamos que você configure o registro em log. Se você quiser permitir que a AWS Control Tower configure uma CloudTrail trilha em nível organizacional e a gerencie para você, escolha Optar por participar. Se você deseja gerenciar o registro com suas próprias CloudTrail trilhas ou com uma ferramenta de registro de terceiros, escolha Optar por não participar. Confirme sua seleção quando solicitado no console. Você pode alterar sua seleção e optar por ou não participar de trilhas de nível organizacional ao atualizar sua landing zone.

Você pode configurar e gerenciar suas próprias CloudTrail trilhas a qualquer momento, incluindo trilhas em nível organizacional e em nível de conta. Se você configurar CloudTrail trilhas duplicadas, poderá incorrer em custos duplicados quando os CloudTrail eventos forem registrados.

### Configurar opcionalmente AWS KMS keys

Se você quiser criptografar e descriptografar seus recursos com uma chave de AWS KMS criptografia, marque a caixa de seleção. Se você tiver chaves existentes, poderá selecioná-las a partir dos identificadores exibidos em um menu suspenso. Você pode gerar uma nova chave escolhendo Criar uma chave. Você pode adicionar ou alterar uma KMS chave sempre que atualizar sua landing zone.

Quando você seleciona Configurar landing zone, o AWS Control Tower realiza uma pré-verificação para validar sua KMS chave. A chave deve atender aos seguintes requisitos:

- Habilitado
- Simétrica
- Não é uma chave multirregional
- Tem as permissões corretas adicionadas à política
- A chave está na conta de gerenciamento

Você pode ver um banner de erro se a chave não atender a esses requisitos. Nesse caso, escolha outra chave ou gere uma chave. Certifique-se de editar a política de permissões da chave, conforme descrito na próxima seção.

### Atualize a política de KMS chaves

Antes de atualizar uma política de KMS chaves, você deve criar uma KMS chave. Para obter mais informações, consulte Criar uma política de chave no Guia do desenvolvedor do AWS Key Management Service .

Para usar uma KMS chave com o AWS Control Tower, você deve atualizar a política de KMS chaves padrão adicionando as permissões mínimas necessárias para AWS Config AWS CloudTrail e. Como prática recomendada, recomendamos que você inclua as permissões mínimas necessárias em qualquer política. Ao atualizar uma política de KMS chaves, você pode adicionar permissões como um grupo em uma única JSON declaração ou linha por linha.

O procedimento descreve como atualizar a política de KMS chaves padrão no AWS KMS console adicionando declarações de política que permitem AWS Config e devem CloudTrail ser usadas AWS KMS para criptografia. As declarações de política exigem que você inclua as seguintes informações:

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— o ID da conta de gerenciamento na qual a AWS Control Tower será configurada.
- **`YOUR-HOME-REGION`**— a região de origem que você selecionará ao configurar a AWS Control Tower.
- **`YOUR-KMS-KEY-ID`**— o ID da KMS chave que será usado com a política.

Para atualizar a política de KMS chaves

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms
2. No painel de navegação, escolha Chaves gerenciadas pelo cliente.
3. Na tabela, selecione a chave que você deseja editar.
4. Na guia Política de chaves, verifique se você pode visualizar a política de chaves. Se você não conseguir visualizar a política principal, escolha Alternar para a visualização da política.
5. Escolha Editar e atualize a política de KMS chaves padrão adicionando as seguintes declarações de política para AWS Config CloudTrail e.

   AWS Config declaração de política

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
```

```
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

CloudTrail declaração de política

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
    }
}
```

6. Escolha Salvar alterações.

### Exemplo de política de KMS chaves

O exemplo de política a seguir mostra como sua política de KMS chaves pode ficar depois de adicionar as declarações de política que concedem AWS Config e CloudTrail as permissões mínimas necessárias. O exemplo de política não inclui sua política de KMS chaves padrão.

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
```

```
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

Para ver outros exemplos de políticas, consulte as páginas a seguir:

- Conceder permissões de criptografia no Guia do AWS CloudTrail usuário.
- Permissões necessárias para a KMS chave ao usar o Service-Linked RoleS3 (Bucket Delivery) no Guia do desenvolvedor.AWS Config

> **Proteja-se contra atacantes**
>
> Ao adicionar determinadas condições às suas políticas, você pode ajudar a evitar um tipo específico de ataque, conhecido como ataque adjunto confuso, que ocorre se uma entidade coagir uma entidade com mais privilégios a realizar uma ação, como a falsificação de identidade entre serviços. Para obter informações gerais sobre as condições da política, consulte tambémEspecificar condições em uma política.

O AWS Key Management Service (AWS KMS) permite criar chaves multirregionais e KMS chaves assimétricas; no entanto, o AWS Control Tower não oferece suporte a chaves multirregionais ou assimétricas. AWSO Control Tower executa uma pré-verificação das chaves existentes. Você pode ver uma mensagem de erro se selecionar uma chave multirregional ou uma chave assimétrica. Nesse caso, gere outra chave para uso com os recursos da AWS Control Tower.

Para obter mais informações sobre AWS KMS, consulte o Guia do AWS KMS desenvolvedor.

Observe que os dados do cliente no AWS Control Tower são criptografados em repouso, por padrão, usando SSE -S3.

Opcionalmente, configure e crie contas de membros personalizadas

Ao seguir o fluxo de trabalho Criar conta para adicionar suas contas de membros, você pode, opcionalmente, especificar um esquema previamente definido para uso no provisionamento de contas de membros personalizadas a partir do console do Control Tower. AWS Você pode personalizar contas posteriormente se não tiver um plano disponível. Consulte Personalize contas com Account Factory Customization (AFC).

## Etapa 3. Revise e configure a landing zone

A próxima seção da configuração mostra as permissões que o AWS Control Tower exige para sua landing zone. Escolha uma caixa de seleção para expandir cada tópico. Você deverá concordar

com essas permissões, que podem afetar várias contas, e que concorde com os Termos de Serviço gerais.

Para finalizar

1. No console, revise as permissões do serviço e, quando estiver pronto, escolha Eu entendo as permissões que a AWS Control Tower usará para administrar AWS recursos e aplicar regras em meu nome.
2. Para finalizar suas seleções e inicializar o lançamento, escolha Configurar landing zone.

Essa série de etapas inicia o processo de configuração do seu landing zone, que pode levar cerca de trinta minutos para ser concluído. Durante a configuração, o AWS Control Tower cria seu nível raiz, a UO de segurança e as contas compartilhadas. Outros AWS recursos são criados, modificados ou excluídos.

> ⚠ Confirmar SNS assinaturas
>
> O endereço de e-mail que você forneceu para a conta de auditoria receberá e-mails de AWS notificação — confirmação de assinatura de todas as AWS regiões suportadas pela AWS Control Tower. Para receber e-mails de conformidade em sua conta de auditoria, você deve escolher o link Confirmar assinatura em cada e-mail de cada AWS região suportada pela AWS Control Tower.

# Comece a usar o AWS Control Tower usando APIs

Esse procedimento de introdução é destinado aos administradores da AWS Control Tower. Esse procedimento requer alguns pré-requisitos e inclui duas etapas principais.

Neste procedimento, você usará o APIs AWS Control Tower e outros AWS serviços para configurar e iniciar uma landing zone. Isso APIs permite que você crie um ambiente AWS Control Tower programaticamente, por meio do AWS CloudFormation console ou do AWS CLI.

Antes de iniciar sua landing zone da AWS Control Tower, execute estas tarefas de pré-requisito:

- Determine a região de origem mais adequada. Para obter mais informações, consulte Dicas administrativas para configuração da landing zone .

- Analise Pré-requisito: verificações automáticas de pré-lançamento para sua conta de gerenciamento para saber mais sobre as verificações automáticas de pré-lançamento que garantem que sua conta de gerenciamento esteja pronta para as mudanças que estabelecem sua landing zone.

Tópicos



## Expectativas para a configuração da landing zone com APIs

O processo de configuração da sua landing zone da AWS Control Tower tem várias etapas. Certos aspectos da sua zona de pouso do AWS Control Tower são configuráveis. Outras opções não podem ser alteradas após a configuração.

Itens principais a serem configurados durante a configuração

- Você pode selecionar seus nomes básicos de UO durante a configuração e também pode alterar os nomes de UO depois de configurar sua landing zone. Por padrão, os Foundational OUs são denominados Security e Sandbox. Para obter mais informações, consulte Diretrizes para configurar um ambiente bem arquitetado.
- Durante a configuração, você pode selecionar nomes personalizados para as contas compartilhadas que a AWS Control Tower cria, chamadas de arquivamento de registros e auditoria por padrão, mas não pode alterar esses nomes após a configuração. (Essa é uma seleção única.)
- Durante a configuração comAPIs, você deve especificar AWS as contas existentes para o AWS Control Tower usar como contas de auditoria e arquivamento de registros. Para especificar AWS

contas existentes, se essas contas tiverem AWS Config recursos existentes, você deverá excluir ou modificar os AWS Config recursos existentes antes de poder inscrever as contas na AWS Control Tower. (Essa é uma seleção única.)

- Se você estiver se configurando pela primeira vez ou se estiver atualizando para a versão 3.0 da landing zone, você pode escolher se deseja permitir que a AWS Control Tower configure uma AWS CloudTrail trilha em nível organizacional para sua organização ou pode optar por não usar trilhas gerenciadas pela Control Tower e gerenciar suas AWS próprias trilhas. CloudTrail Você pode ativar ou desativar as trilhas de nível organizacional gerenciadas pela AWS Control Tower sempre que atualizar sua landing zone.
- Opcionalmente, você pode definir uma política de retenção personalizada para seu bucket de log e bucket de acesso ao log do Amazon S3 ao configurar ou atualizar sua landing zone.

Opções de configuração que não podem ser desfeitas

- Você não pode mudar sua região de origem depois de configurar sua landing zone.
- Se você estiver provisionando contas comVPCs, elas não VPC CIDRs poderão ser alteradas depois de criadas.

As próximas seções fornecem os pré-requisitos e as etapas de configuração em detalhes, com explicações e ressalvas. Consulte mais exemplos de código em Exemplos: configure uma landing zone do AWS Control Tower somente com APIs.

## Etapa 1: configure sua landing zone

O processo de configuração da sua landing zone da AWS Control Tower tem várias etapas. Certos aspectos da sua zona de pouso do AWS Control Tower são configuráveis, mas outras opções não podem ser alteradas após a configuração. Para saber mais sobre essas considerações importantes antes de lançar sua landing zone, Expectativas para a configuração da landing zone revise.

Antes de usar a zona de pouso da AWS Control TowerAPIs, você deve primeiro ligar APIs para outros AWS serviços para configurar sua zona de pouso antes do lançamento. O processo inclui três etapas principais:

- criando uma nova AWS Organizations organização,
- configurando os endereços de e-mail da sua conta compartilhada,
- e criar uma IAM função ou usuário do IAM Identity Center com as permissões necessárias para ligar para a landing zoneAPIs.

Etapa 1. Crie a organização que conterá sua landing zone:

1. Ligue para AWS Organizations `CreateOrganization` API e ative todos os recursos para criar a OU básica. AWSInicialmente, a Control Tower chama isso de Security OU. Essa OU de segurança contém suas duas contas compartilhadas, que por padrão são chamadas de conta de arquivamento de log e conta de auditoria.

   ```
   aws organizations create-organization --feature-set ALL
   ```

   AWSA Control Tower pode configurar um ou mais adicionais OUs. Recomendamos que você provisione pelo menos uma OU adicional em sua landing zone, além da OU de segurança. Se essa OU adicional for destinada a projetos de desenvolvimento, recomendamos que você a nomeie como Sandbox OU, conforme indicado noAWS estratégia de várias contas para sua zona de pouso da AWS Control Tower.

Etapa 2. Provisione contas compartilhadas, se necessário:

Para configurar sua landing zone, o AWS Control Tower requer dois endereços de e-mail. Se você estiver usando o landing zone APIs para configurar o AWS Control Tower pela primeira vez, deverá usar as AWS contas existentes de segurança e arquivamento de registros. Você pode usar os endereços de e-mail atuais dos existentes Contas da AWS. Cada um desses endereços de e-mail servirá como uma caixa de entrada colaborativa — uma conta de e-mail compartilhada — destinada aos vários usuários da sua empresa que realizarão trabalhos específicos relacionados à AWS Control Tower.

Para começar a configurar uma nova landing zone, se você não tiver AWS contas existentes, você pode provisionar as contas de segurança e arquivamento AWS de registros usando AWS Organizations APIs.

1. Ligue AWS Organizations `CreateAccount` API para o para criar a conta de arquivamento de registros e a conta de auditoria na OU de segurança.

   ```
   aws organizations create-account --email mylog@example.com --account-name "Logging
    Account"
   ```

   ```
   aws organizations create-account --email mysecurity@example.com --account-name
    "Security Account"
   ```

2. (Opcional) Verifique o status da `CreateAccount` operação usando AWS Organizations `DescribeAccount` API o.

Etapa 3. Crie as funções de serviço necessárias

Crie as seguintes funções IAM de serviço que permitam que a AWS Control Tower realize as API chamadas necessárias para configurar sua landing zone:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Para obter mais informações sobre essas funções e suas políticas, consulteUsando políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower.

Para criar uma IAM função:

1. Crie uma IAM função com as permissões necessárias para chamar toda a landing zoneAPIs. Como alternativa, você pode criar um usuário do IAM Identity Center e atribuir as permissões necessárias.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListLandingZoneOperations",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
```

```
                "organizations:*",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

## Etapa 2: inicie sua landing zone

O AWS Control Tower `CreateLandingZone` API exige uma versão da landing zone e um arquivo de manifesto como parâmetros de entrada. Você pode usar o arquivo de manifesto para configurar os seguintes recursos:

- Opcionalmente, configure a retenção de registros
- Opcionalmente, Conta da AWS autogerencie o acesso
- Opcionalmente, configure trilhas AWS CloudTrail
- Configurar opcionalmente AWS KMS keys

Depois de compilar seu arquivo de manifesto, você está pronto para criar uma nova landing zone.

> **Note**
>
> AWSO Control Tower não suporta o controle de negação de região APIs ao ser usado para configurar e lançar uma landing zone. Depois de iniciar com sucesso sua landing zone usandoAPIs, você pode usar o console AWS Control Tower para configurar o controle de negação de região.

1. Ligue para a AWS Control Tower `CreateLandingZone`API. Isso API requer uma versão do landing zone e um arquivo de manifesto como entrada.

```
aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
LandingZoneManifest.json"
```

Exemplo de manifesto LandingZoneManifest.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
```

```
        "accountId": "333333333333"
    },
    "accessManagement": {
        "enabled": true
    }
}
```

> **Note**
>
> Conforme mostrado no exemplo, as SecurityRoles contas AccountIdfor the CentralizedLogging e devem ser diferentes.

Saída:

```
{
   "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

2. Ligue `GetLandingZoneOperation` API para o para verificar o status da `CreateLandingZone` operação. O `GetLandingZoneOperation` API retorna um status de`SUCCEEDED`,`FAILED`, ou`IN_PROGRESS`.

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-
eXXX-4XXX-aXXX-44XXXXXXXXXX"
```

Saída:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. Quando o status retornar como`SUCCEEDED`, você pode ligar `GetLandingZone` API para o para revisar a configuração da landing zone.

```
aws controltower get-landing-zone --landing-zone-identifier "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Saída:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
```

```
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

## Identifique sua landing zone

Ligar `ListLandingZones` pode ajudar você a determinar se sua conta já está configurada com o AWS Control Tower. Isso API retorna um identificador de zona de pouso (ARN) em qualquer região comercial, independentemente da região de origem da zona de pouso. ARNsAs zonas de pouso são exclusivas regionalmente.

```
aws controltower list-landing-zones --region us-east-1
```

Para regiões opcionais, `ListLandingZones` API só retornará o identificador da landing zone se você ligar para a API mesma região da região API de origem. Por exemplo, se sua zona de pouso estiver configurada em af-south-1 e você `ListLandingZones` ligar para af-south-1, ela retornará o identificador da zona de pouso. API Se sua zona de pouso estiver configurada em af-south-1 e você **`ListLandingZones`** ligar para ap-east-1, ela não retornará o identificador da zona de pouso. API

Saída:

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

## Atualize sua landing zone

Quando uma nova versão da zona de pouso estiver disponível, ou para fazer outras atualizações na configuração da sua zona de pouso, você pode chamar o `UpdateLandingZone` API e referenciar

um arquivo de manifesto atualizado. Isso API retorna um`OperationIdentifier`, que você pode usar ao chamar o `GetLandingZoneOperation` API para verificar o status da operação de atualização.

Para atualizar a landing zone

1. Ligue para a AWS Control Tower `UpdateLandingZone` API e consulte a versão atualizada do landing zone ou seu manifesto atualizado.

```
aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
 --manifest file://LandingZoneManifest.json
```

LandingZoneManifest.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
```

```
   "accessManagement": {
        "enabled": true
   }
}
```

Saída:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> Opcionalmente, registre novamente a OU para atualizar contas
>
> Para a AWS Control Tower registrada OUs com menos de 300 contas, você pode usar o console da AWS Control Tower, acessar a página da OU no painel e selecionar Registrar novamente a OU para atualizar as contas nessa OU.

## Redefina a landing zone para resolver o desvio

Quando você cria sua zona de pouso, a zona de pouso e todas as unidades organizacionais (OUs), contas e recursos estão em conformidade com as regras de governança impostas pelos controles escolhidos. À medida que você e os membros da sua organização usam o landing zone, mudanças nesse status de conformidade podem ocorrer. Essas mudanças são chamadas de deriva.

Para identificar se sua landing zone está à deriva, você pode ligar para o. `GetLandingZone` API Isso API retorna o status de deriva da zona de pouso de `DRIFTED` ou`IN_SYNC`.

Para resolver o desvio em sua zona de pouso, você pode usar o `ResetLandingZone` API para redefinir a zona de pouso à configuração original. Por exemplo, o AWS Control Tower ativa o IAM Identity Center por padrão para ajudá-lo a gerenciar seu Contas da AWS-- mas se você configurar os parâmetros originais da landing zone com o IAM Identity Center desativado, a chamada `ResetLandingZone` manterá essa configuração desativada do IAM Identity Center.

Você só pode usar o `ResetLandingZone` API se estiver usando a versão mais recente disponível do landing zone. Você pode ligar para `GetLandingZone` API e comparar a versão do seu landing zone com a versão mais recente disponível. Se necessário, você pode fazer com Atualize sua landing zone que seu landing zone use a versão mais recente disponível. Nesses exemplos, estamos usando a versão 3.3 como a versão mais recente.

1. Ligue para `GetLandingZone` API o. Se API retornar um status de deriva de`DRIFTED`, sua landing zone está em deriva.
2. Ligue `ResetLandingZone` API para o para redefinir sua landing zone para a configuração original.

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Saída:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Note**
>
> A redefinição da zona de pouso não atualiza a versão da zona de pouso. Consulte Atualize sua landing zone para obter detalhes sobre a atualização da versão do landing zone.

## Desative sua landing zone

O processo de limpeza de todos os recursos de uma zona de pouso é chamado de descomissionamento de uma zona de pouso.

> **Important**
>
> Recomendamos veementemente a realização deste processo de desativação exclusivamente se você pretende parar de usar a zona de destino. Não é possível recriar uma zona de destino existente depois de sua desativação.

Para obter mais detalhes sobre o descomissionamento de uma landing zone, incluindo informações importantes sobre como a AWS Control Tower lida com seus dados e os existentes AWS Organizations, revise. Passo a passo: Descomissione uma zona de pouso do AWS Control Tower

Para descomissionar uma landing zone, ligue `DeleteLandingZone`API. Isso API retorna um`OperationIdentifier`, que você pode usar ao chamar o `GetLandingZoneOperation` API para verificar o status da operação de exclusão.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

Saída:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

## Visualize o status das operações da sua landing zone

A `ListLandingZoneOperations` API permite que você visualize o status das operações do AWS Control Tower que realizam ações na sua landing zone.

Para obter mais informações sobre essa operação de API, consulte ListLandingZoneOperations.

### ListLandingZoneOperations

Exemplo de entrada e saída para **`ListLandingZoneOperations`**.

Este exemplo mostra como chamar a API sem parâmetros.

```
aws controltower --region us-east-1 list-landing-zone-operations

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
```

```
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

Este exemplo mostra como chamar a API e especificar o número máximo de resultados.

```
aws controltower --region us-east-1 list-landing-zone-operations --max-results 1

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ],
    "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}
```

Este exemplo mostra como chamar a API e obter um resultado paginado com. `nextToken`

```
aws controltower --region us-east-1 list-landing-zone-operations --next-token
 AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
    "landingZoneOperations": [
        {
```

```
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

Este exemplo mostra como chamar a API com um filtro.

```
aws controltower --region us-east-1 list-landing-zone-operations --filter '{"types":
["CREATE"],"statuses":["FAILED"]}'

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

## Exemplos: configure uma landing zone do AWS Control Tower somente com APIs

Este guia de exemplos é um documento complementar. Para obter explicações, ressalvas e mais informações, consulte Introdução ao AWS Control Tower usando APIs.

Pré-requisitos

Antes de criar uma landing zone do AWS Control Tower, você deve criar uma organização, duas contas compartilhadas e algumas funções do IAM. Este tutorial passo a passo inclui essas etapas, com exemplos de comandos e saídas da CLI.

Etapa 1. Crie a organização e as duas contas necessárias.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

Etapa 2. Crie as funções necessárias do IAM.

`AWSControlTowerAdmin`

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
```

```
            "Resource": "*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

### AWSControlTowerCloudTrailRole

```
cat <<EOF >cloudtrail_trust.json
        {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
```

```
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

### AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Etapa 3. Obtenha os IDs da conta e gere o arquivo de manifesto do landing zone.

Os dois primeiros comandos no exemplo a seguir armazenam as IDs das contas que você criou na Etapa 1 em variáveis. Essas variáveis então ajudam a gerar o arquivo de manifesto do landing zone.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
```

```
   "centralizedLogging": {
        "accountId": "$log_account_id",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "$sec_account_id"
   },
   "accessManagement": {
        "enabled": true
   }
}
EOF
```

Etapa 4. Crie a landing zone com a versão mais recente.

Você deve configurar a landing zone com o arquivo de manifesto e a versão mais recente. Este exemplo mostra a versão 3.3.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

A saída conterá um arn e um OperationIdentifier, conforme mostrado no exemplo a seguir.

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

Etapa 5. (Opcional) Acompanhe o status da operação de criação da sua landing zone configurando um loop.

Para rastrear o status, use o OperationIdentifier da saída do `create-landing-zone` comando anterior.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

Saída de status da amostra:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
}
```

Você pode usar o script de exemplo a seguir para ajudá-lo a configurar um loop, que relata o status da operação repetidamente, como um arquivo de log. Então você não precisa continuar digitando o comando.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

Para mostrar informações detalhadas sobre sua landing zone

Etapa 1. Encontre o ARN da landing zone

```
aws --region us-west-1 controltower list-landing-zones
```

A saída incluirá o identificador da landing zone, conforme mostrado no exemplo de saída a seguir.

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

Etapa 2. Obtenha as informações

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

Aqui está um exemplo do tipo de saída que você pode ver:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
```

```
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

Etapa 6. (Opcional) Chame a **`ListLandingZoneOperations`** API para ver o status de qualquer operação que mude sua landing zone.

Para rastrear o status de qualquer operação de landing zone, você pode chamar a ListLandingZoneOperations API.

## Inicie uma landing zone usando AWS CloudFormation

Você pode configurar e iniciar uma landing zone por meio do AWS CloudFormation console ou do AWS CLI. AWS CloudFormation Esta seção fornece instruções e exemplos para lançar uma landing zone usando APIs through AWS CloudFormation.

Tópicos

- Pré-requisitos para lançar uma landing zone usando AWS CloudFormation
- Crie uma nova landing zone usando AWS CloudFormation
- Gerencie uma landing zone existente usando AWS CloudFormation

### Pré-requisitos para lançar uma landing zone usando AWS CloudFormation

1. A partir do AWS CLI, use o AWS Organizations `CreateOrganization` API para criar uma organização e ativar todos os recursos.

   Para obter instruções mais detalhadas, revise Etapa 1: configure sua landing zone .
2. No AWS CloudFormation console ou usando o AWS CLI, implante um AWS CloudFormation modelo que crie os seguintes recursos na conta de gerenciamento:
   - Conta do Log Archive (às vezes chamada de conta “Logging”)
   - Conta de auditoria (às vezes chamada de conta “Segurança”)
   - As funções AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations, e AWSControlTowerStackSetRolede serviço.

Para obter informações sobre como a AWS Control Tower usa essas funções para realizar API chamadas na zona de pouso, consulte Etapa 1: Configurar sua zona de pouso.

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
```

```
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
```

```
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
```

```
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

## Crie uma nova landing zone usando AWS CloudFormation

No AWS CloudFormation console ou usando o AWS CLI, implante o AWS CloudFormation modelo a seguir para criar uma landing zone.

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
```

```
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
          enabled: true
```

### Gerencie uma landing zone existente usando AWS CloudFormation

Você pode usar AWS CloudFormation para gerenciar uma zona de pouso que você já lançou importando a zona de pouso em uma AWS CloudFormation pilha nova ou existente. Revise a incorporação dos recursos existentes ao CloudFormation gerenciamento para obter detalhes e instruções.

Para detectar e resolver a deriva em uma landing zone, você pode usar o console AWS Control Tower AWS CLI, o ou o. `ResetLandingZone`API

## Próximas etapas

Agora que sua landing zone está configurada, ela está pronta para uso.

Para saber mais sobre como você pode usar o AWS Control Tower, consulte os seguintes tópicos:

- Para ver as melhores práticas administrativas, consulte Melhores práticas.
- Você pode configurar usuários e grupos do IAM Identity Center com funções e permissões específicas. Para obter recomendações, consulte Recomendações para configurar grupos, funções e políticas .
- Para começar a inscrever organizações e contas de suas AWS Organizations implantações, consulte Governar organizações e contas existentes.
- Seus usuários finais podem provisionar suas próprias AWS contas na sua landing zone usando o Account Factory. Para ter mais informações, consulte Permissões para configurar e provisionar contas.
- Para garantirValidação de conformidade para AWS Control Tower, seus administradores de nuvem central podem revisar os arquivos de log na conta do Log Archive, e auditores terceirizados designados podem revisar as informações de auditoria na conta de auditoria (compartilhada), que é membro da OU de segurança.
- Para saber mais sobre os recursos do AWS Control Tower, consulte Informações relacionadas.
- Experimente visitar uma lista selecionada de YouTube vídeos que explicam mais sobre como usar a funcionalidade do AWS Control Tower.
- De tempos em tempos, talvez seja necessário atualizar sua zona de pouso para obter as atualizações de back-end mais recentes, os controles mais recentes e manter sua zona up-to-date de pouso. Para ter mais informações, consulte Gerenciamento de atualizações de configuração no AWS Control Tower.

- Se você encontrar problemas ao usar o AWS Control Tower, consulteSolução de problemas.

> **Important**
>
> Se você ainda não habilitou o MFA para o usuário root da sua conta, faça isso agora. Para obter mais informações sobre as melhores práticas para o usuário raiz, consulte Práticas recomendadas para proteger o usuário raiz da sua conta.

# Limitações e cotas na AWS Control Tower

Este capítulo aborda as limitações e cotas do AWS serviço que você deve ter em mente ao usar o AWS Control Tower. Se você não conseguir configurar sua landing zone devido a um problema de cota de serviço, entre em contato AWS Support.

Para obter mais informações sobre limitações específicas dos controles, consulteLimitações de controle.

> O guia de referência de controles
>
> Informações detalhadas sobre os controles da AWS Control Tower foram transferidas para o Guia de referência dos controles da AWS Control Tower.

## Limitações conhecidas na AWS Control Tower

Esta seção descreve as limitações conhecidas e os casos de uso sem suporte no AWS Control Tower.

- AWSO Control Tower tem limitações gerais de simultaneidade. Em geral, uma operação por vez é permitida. Duas exceções a essa limitação são permitidas:
  - Os controles opcionais podem ser ativados e desativados simultaneamente, por meio de um processo assíncrono. Até cem (100) operações relacionadas ao controle por vez podem estar em andamento, no total, independentemente de serem chamadas do console ou de umAPI. Dessas 100 operações, até 20 por vez podem ser operações de controle proativas.
  - As contas podem ser provisionadas, atualizadas e inscritas simultaneamente no Account Factory, por meio de um processo assíncrono, com até cinco (5) operações relacionadas à conta em andamento simultaneamente. O não gerenciamento de contas deve ser realizado uma conta por vez.
- Os endereços de e-mail das contas compartilhadas na UO de Segurança podem ser alterados, mas você deve atualizar sua landing zone para ver essas alterações no console do AWS Control Tower.
- Um limite de cinco (5) SCPs por UO se aplica à OUs sua landing zone da AWS Control Tower.
- AWSO Control Tower suporta até 10.000 contas na organização da sua zona de pouso, divididas entre todas as suasOUs.

- As contas existentes OUs com mais de 1000 contas diretamente aninhadas não podem ser registradas ou registradas novamente no AWS Control Tower. Para obter mais informações sobre limitações no registroOUs, consulteLimitações com base nos AWS serviços subjacentes.
- As personalizações do AWS Control Tower (cFct) não estão disponíveis nestes Regiões da AWS, porque algumas dependências não estão disponíveis:
  - Região da Europa (Zurique), eu-central-2
  - Região da Europa (Espanha), eu-south-2
  - Oeste do Canadá (Calgary)

  Você pode implantar e gerenciar recursos nessas regiões com o cFCT, se você implantar o cFCT na sua região de origem da AWS Control Tower, mas não pode criar o cFCT nessas regiões.
- AWSO Control Tower Account Factory for Terraform (AFT) não está disponível no seguinte Regiões da AWS, porque algumas dependências não estão disponíveis:
  - Região da Europa (Zurique), eu-central-2
  - Região da Europa (Espanha), eu-south-2
  - Oeste do Canadá (Calgary)
- AWSO Control Tower Account Factory for Terraform (AFT) não pode ser implantado por novos AFT clientes nas seguintes regiões, porque o AWS CodeStar Connections não está disponível para conexão com um sistema de controle de versão de terceiros ()VCS:
  - Ásia-Pacífico (Hong Kong), África (Cidade do Cabo), Oriente Médio (Bahrein), Europa (Zurique), Ásia-Pacífico (Jacarta), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Osaka), Ásia-Pacífico (Melbourne), Israel (Tel Aviv), Europa (Espanha) e Oriente Médio () UAE
- As seguintes regiões não oferecem suporte ao IAMIdentity Center.
  - Região do Oriente Médio (UAE), me-central-1
  - Região Ásia-Pacífico (Hyderabad), ap-south-2
  - Oeste do Canadá (Calgary), ca-west-1

  Para obter mais informações Regiões da AWS e suporte para o IAM Identity Center, consulte Regiões e endpoints no Guia do usuário do AWS Identity and Access Management.
- As seguintes regiões não oferecem suporte AWS Service Catalog.
  - Oeste do Canadá (Calgary), ca-west-1

Para obter mais informações sobre a funcionalidade AWS Control Tower em regiões que não oferecem suporte AWS Service Catalog, consulteAWSControl Tower disponível em AWS Oeste do Canadá (Calgary).

- Ao chamar um controle API para ativar ou desativar um controle, o limite `EnableControl` e as `DisableControl` atualizações na AWS Control Tower são cem (100) operações simultâneas. Dez operações (10) podem estar em andamento simultaneamente, com as demais operações na fila. Talvez seja necessário ajustar seu código para aguardar a conclusão.
- Dentro do limite geral de 100 operações de controle, até 20 operações por vez podem ser operações de controle proativas.
- Ao provisionar contas por meio de Account Factory Customizations (AFC), com blueprints baseados no Terraform, você pode implantar esses blueprints em apenas um. Região da AWS Por padrão, o AWS Control Tower é implantado na região de origem.

# Solicitar um aumento da cota

O console Service Quotas fornece informações sobre as cotas da AWS Control Tower. É possível usar o console do serviço de cotas para visualizar cotas padrão ou solicitar aumentos de cota para cotas ajustáveis.

As cotas a seguir podem ser visualizadas por meio do console Service Quotas

- Cota de operações de conta simultânea: o número máximo de operações de conta simultânea que podem ser executadas ao mesmo tempo. Padrão: 5, máximo: 10, ajustável
- Número de contas em uma única OU: o número máximo de contas gerenciadas da AWS Control Tower que podem estar presentes em uma OU. Se você adicionar contas além desse limite, o processo de registro da OU no AWS Control Tower não poderá ser executado. Para saber mais sobre o número de contas por UO, consulte Limitações com base nos AWS serviços subjacentes a documentação da AWS Control Tower. Padrão: 1000, não ajustável.
- Operações simultâneas para unidades organizacionais (OUs): o número máximo de operações simultâneas relacionadas à OU que podem ser executadas ao mesmo tempo. Padrão: 1, não ajustável.

Por exemplo, você pode solicitar um aumento de cota de cinco de até dez operações simultâneas relacionadas à conta. Algumas características de desempenho da AWS Control Tower podem mudar após o aumento da cota. Por exemplo, pode levar mais tempo para atualizar uma OU quando você

tem mais contas nela. Ou pode levar mais tempo para concluir uma ação em uma OU com cinco SCPs do que com trêsSCPs.

> **Note**
>
> Uma solicitação de aumento de cota de serviço pode exigir até dois dias antes de entrar em vigor. Não se esqueça de solicitar o aumento da cota na sua região de origem da AWS Control Tower.

Como alternativa, você pode entrar em contato com o AWS Support para solicitar um aumento de cota para alguns recursos na AWS Control Tower. Ou você pode assistir ao vídeo a seguir e aprender como automatizar determinados aumentos de cota de serviço.

Vídeo: Automatize as solicitações de aumento de cota de serviço em serviços relacionados ao AWS Control Tower

Este vídeo (7:24) descreve como automatizar o aumento da cota de serviço para AWS serviços relacionados e integrados, com base em implantações na Control Tower. AWS Também mostra como automatizar a inscrição de novas contas no suporte AWS corporativo da sua organização. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Passo a passo em vídeo dos aumentos de cotas na Control TowerAWS.

Ao provisionar novas contas nesse ambiente, você pode usar eventos de ciclo de vida para acionar solicitações automatizadas de aumentos de cota de serviço, conforme especificado. Regiões da AWS

Mais informações sobre AWS cotas estão disponíveis na Referência AWS Geral.

## Limitações de controle

AWSO Control Tower ajuda você a manter um ambiente seguro com várias contas AWS por meio de controles, que são implementados de várias formas, como políticas de controle de serviço (SCPs), AWS Config regras e AWS CloudFormation ganchos.

> **O guia de referência de controles**
>
> Informações detalhadas sobre os controles da AWS Control Tower foram transferidas para o Guia de referência dos controles da AWS Control Tower.

Se você modificar recursos da AWS Control Tower, como umSCP, ou remover qualquer AWS Config recurso, como um gravador ou agregador do Config, a Control Tower AWS não poderá mais garantir que os controles estejam funcionando conforme projetado. Portanto, a segurança do seu ambiente de várias contas pode estar comprometida. O modelo de segurança de responsabilidade AWS compartilhada é aplicável a quaisquer alterações que você possa fazer.

> **Note**
>
> AWSO Control Tower ajuda a manter a integridade do seu ambiente redefinindo os SCPs controles preventivos para a configuração padrão quando você atualiza sua landing zone. As alterações que você possa ter feito SCPs são substituídas pela versão padrão do controle, por design.

Limitações por região

Alguns controles na AWS Control Tower não operam em determinados Regiões da AWS locais onde a AWS Control Tower está disponível, porque essas regiões não oferecem suporte à funcionalidade subjacente necessária. Como resultado, quando você implanta esse controle, ele pode não estar operando em todas as regiões que você governa com a AWS Control Tower. Essa limitação afeta certos controles de detetive, certos controles proativos e certos controles no Security Hub Service-Managed Standard: Control Tower. AWS Para obter mais informações sobre a disponibilidade regional, consulte os controles do Security Hub. Consulte também a documentação da lista de serviços regionais e a documentação de referência dos controles do Security Hub.

O comportamento de controle também é limitado no caso de governança mista. Para obter mais informações, consulte Evite governança mista ao configurar regiões.

Para obter mais informações sobre como a AWS Control Tower gerencia as limitações de regiões e controles, consulteConsiderações sobre a ativação de regiões opcionais AWS.

> **Note**
>
> Para obter as informações mais atualizadas sobre controles e suporte regional, recomendamos que você ligue para as `ListControls`APIoperações `GetControl`e.

## Encontre controles e regiões disponíveis

Você pode ver as regiões disponíveis para cada controle no console AWS Control Tower. Você pode visualizar as regiões disponíveis programaticamente com o `GetControl`e do Catálogo `ListControls`APIsde AWS Controle.

Consulte também a tabela de referência dos controles da AWS Control Tower e regiões suportadas, Control availability by Region, no AWSControl Tower Controls Reference Guide.

Não compatível com o padrão AWS Security Hub gerenciado Regiões da AWS por serviços: Control Tower AWS

Para obter informações sobre AWS Security Hub controles do Service-Managed Standard: AWS Control Tower que não são suportados em determinadas regiões Regiões da AWS, consulte “Regiões não suportadas” no padrão do Security Hub.

Os itens a seguir Regiões da AWS, como região de origem, não oferecem suporte à implantação de controles proativos. Você pode implantar controles proativos para governar essas regiões se implantar os controles de uma região de origem diferente que ofereça suporte a controles proativos.

- Oeste do Canadá (Calgary)

A tabela a seguir mostra controles proativos que não são suportados em alguns Regiões da AWS.

| Identificador de controle | Regiões não implantáveis |
| --- | --- |
| `CT.DAX.PR.2` | ca-west-1, us-west-1 |
| `CT.REDSHIFT.PR.5` | ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-4, ca-west-1, eu-central-2, eu-sul-2, il-central-1, me-central-1 |

A tabela a seguir mostra os controles de detetive da AWS Control Tower que não são suportados em alguns Regiões da AWS.

| Identificador de controle | Regiões não implantáveis |
| --- | --- |
| AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED | ap-nordeste-3, ap-sudeste-3, ap-southeast-3, ap-southeast-4, ca-west-1, il-central-1 |
| AWS-GR_DMS_REPLICATION_NOT_PUBLIC | af-south-1, ap-south-2, ap-southeast-3, ap-southeast-4, ca-west-1, eu-central-2, eu-sul-1, eu-central-2, eu-south-1, eu-south-2, eu-south-2, -central-1, me-central-1 |
| AWS-GR_EBS_OPTIMIZED_INSTANCE | ca-west-1 |
| AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK | eu-south-2 |
| AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP | ap-northeast-3 |
| AWS-GR_EC2_VOLUME_INUSE_CHECK | ca-west-1 |
| AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS | ca-west-1 |
| AWS-GR_ELASTICSEARCH_IN_VPC_ONLY | ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-4, ca-west-1, eu-central-2, eu-south-2, il-central-1 |
| AWS-GR_EMR_MASTER_NO_PUBLIC_IP | af-south-1, ap-nordeste-3, ap-south-2, ap-south-2, ap-southeast-3, ap-southeast-4, ca-west-1, eu-central-2, eu-sul-1, eu-central-2, eu-sul-1 eu-sul-2, il-central-1, eu-central-1, me-central-1 |
| AWS-GR_ENCRYPTED_VOLUMES | af-south-1, ap-northeast-3, eu-sul-1, il-central-1 |
| AWS-GR_IAM_USER_MFA_ENABLED | ap-south-2, ap-southeast-4, ca-west-1, eu-central-2, eu-south-2, il-central-1, me-central-1 |

| Identificador de controle | Regiões não implantáveis |
| --- | --- |
| AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED | eu-south-2 |
| AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS | ap-south-2, ap-southeast-4, ca-west-1, eu-central-2, eu-south-2, il-central-1, me-central-1 |
| AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW | ap-northeast-3, ap-south-2, ap-southeast-3, ap-west-1, eu-south-2 |
| AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK | ap-south-2, eu-south-2 |
| AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED | af-south-1, ap-southeast-4, eu-central-2, eu-sul-1, eu-south-2, eu-central-1 |
| AWS-GR_RDS_STORAGE_ENCRYPTED | eu-central-2, eu-south-2 |
| AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK | ap-south-2, ap-southeast-3, ap-west-1, eu-south-2 |
| AWS-GR_RESTRICTED_SSH | af-south-1, eu-south-1 |
| AWS-GR_ROOT_ACCOUNT_MFA_ENABLED | ca-west-1, il-central-1, me-central-1 |
| AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC | eu-central-2, eu-sul-2, il-central-1 |
| AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS | af-south-1, ap-nordeste-3, ap-south-2, ap-south-2, ap-southeast-3, ap-southeast-4, ca-west-1, eu-central-2, eu-sul-1, eu-central-2, eu-sul-1 eu-sul-2, il-central-1, eu-central-1, me-central-1 |
| AWS-GR_SSM_DOCUMENT_NOT_PUBLIC | ca-west-1, il-central-1 |
| AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED | ap-northeast-3 |

# Limitações com base nos AWS serviços subjacentes

Esta página descreve as limitações que você pode encontrar devido a limitações em outros AWS serviços e como a AWS Control Tower funciona com esses serviços.

## Diretrizes gerais

Como regra geral, esperamos que o número de contas suportadas ao registrar uma OU diminua à medida que você aumenta o número de regiões governadas e o número de controles ativados para essa OU. Essas diretrizes gerais pressupõem que você tenha 15 controles opcionais ativados. Se você tiver mais ou menos controles habilitados em sua OU, os limites de contas por OU serão diferentes ao se registrar.

- Com 15 regiões governadas, OUs há suporte para até 1000 contas.
- Com 16 a 21 regiões governadas, o tamanho máximo de OU suportado está na faixa de 600 a 1000 contas.
- Com 22 regiões governadas, há OUs suporte para até 680 contas.
- Com 23 ou mais regiões governadas, o tamanho máximo de OU suportado é inferior a 680 contas.

## Em caso de erro

Se o registro falhar, você pode tentar registrar novamente a OU. Além disso, você pode diminuir a OU usando uma OU aninhada ou transferindo contas para outra OU.

> **Note**
>
> Os controles obrigatórios que o AWS Control Tower sempre impõe não são contabilizados no número de controles que você ativou em uma OU, para fins de registro.

## AWS CloudFormation limitações do conjunto de pilhas

Se você planeja registrar um grande número de contas em várias Regiões da AWS, pode encontrar limites criados por conjuntos de AWS CloudFormation pilhas no tamanho geral de uma organização. Você pode estimar a limitação com esta fórmula:

Número de contas gerenciadas na organização x Número de regiões governadas <= 150.000

Essa limitação se torna aparente durante o processo de registro da OU. Por exemplo, se 15 regiões forem governadas e 15 controles opcionais estiverem habilitados, o limite para registrar a OU será de 1.000 contas. No entanto, se você precisar se registrar OUs com mais de 1.000 contas ou se tiver um grande número de controles opcionais ativados, deverá reduzir o número de regiões governadas para menos de 15. Essa redução se deve às limitações do conjunto de pilhas.

AWS Config Limitações

Se você planeja se registrar OUs com um grande número de contas, poderá encontrar limites com o número máximo de contas que AWS Config podem ser criadas ou excluídas a cada semana, em todos os agregadores. As contas inscritas não contam para esse limite: você pode inscrever até 1.000 novas contas no AWS Control Tower a cada semana.

Limitações iniciais para contas e regiões optativas

Se você planeja se registrar OUs com um grande número de contas em várias regiões optativas pela primeira vez, poderá encontrar limitações devido às cotas de gerenciamento de contas, o que pode levar a uma latência prolongada. Podem ocorrer erros durante o registro da OU devido à latência.

# Diferenças regionais na funcionalidade do AWS Control Tower

Existem certas diferenças no comportamento do AWS Control Tower em toda parte Regiões da AWS, porque o AWS Control Tower orquestra o comportamento de outros AWS serviços. Por exemplo: .

- AWS Service Catalog não está disponível em todos os Regiões da AWS lugares onde o AWS Control Tower está disponível, o que muda o comportamento do Account Factory nessas regiões.
- Em determinadas regiões, o Account Factory Customizations (AFC) não está disponível porque o Service Catalog não está disponível para oferecer suporte à funcionalidade subjacente dos blueprints.
- Alguns controles não estão disponíveis em todos Regiões da AWS devido à falta de funcionalidade subjacente.
- AFT e cFct não estão disponíveis em todos Regiões da AWS devido à falta de funcionalidade subjacente.

Para fazer a melhor determinação de comportamento para seu ambiente do AWS Control Tower, verifique sua região de origem. Em seguida, avalie os itens a seguir. Para obter mais detalhes, consulte Limitações e cotas no AWS Control Tower.

- Está AWS Service Catalog disponível na região de origem desejada?
- Os controles de que você precisa estão disponíveis? Consulte Limitações de controle.
- O IAM Identity Center está disponível na região de origem desejada?

# Novo: Guia de referência do AWS Control Tower Controls

As informações sobre controles na AWS Control Tower foram transferidas para um novo guia, o AWS Control Tower Controls Reference Guide.

# Práticas recomendadas para administradores da AWS Control Tower

Este tópico é destinado principalmente aos administradores de contas de gerenciamento.

Os administradores da conta de gerenciamento são responsáveis por explicar algumas tarefas que os controles da AWS Control Tower impedem que seus administradores de contas de membros realizem. Este tópico descreve algumas das melhores práticas e procedimentos para transferir esse conhecimento e fornece outras dicas para configurar e manter seu ambiente AWS Control Tower de forma eficiente.

## Explicando o acesso aos usuários

O console AWS Control Tower está disponível somente para usuários com as permissões de administrador da conta de gerenciamento. Somente esses usuários podem realizar trabalhos administrativos em sua landing zone. De acordo com as melhores práticas, isso significa que a maioria dos seus usuários e administradores de contas de membros nunca verão o console do AWS Control Tower. Como membro do grupo de administradores da conta de gerenciamento, é sua responsabilidade explicar as seguintes informações aos usuários e administradores de suas contas de membros, conforme apropriado.

- Explique a quais AWS recursos os usuários e administradores têm acesso na landing zone.
- Liste os controles preventivos que se aplicam a cada unidade organizacional (OU) para que os outros administradores possam planejar e executar suas AWS cargas de trabalho adequadamente.

## Explicando o acesso aos recursos

Alguns administradores e outros usuários podem precisar de uma explicação sobre os AWS recursos aos quais eles têm acesso na sua landing zone. Esse acesso pode incluir acesso programático e acesso com base no console. De um modo geral, o acesso de leitura e gravação aos AWS recursos é permitido. Para realizar trabalhos internos AWS, seus usuários precisam de algum nível de acesso aos serviços específicos de que precisam para realizar seus trabalhos.

Alguns usuários, como seus AWS desenvolvedores, talvez precisem conhecer os recursos aos quais têm acesso para criar soluções de engenharia. Outros usuários, como os usuários finais dos

aplicativos executados nos AWS serviços, não precisam conhecer AWS os recursos em sua landing zone.

AWS oferece ferramentas para identificar o escopo do acesso de um usuário aos AWS recursos. Depois de identificar o escopo do acesso de um usuário, você poderá compartilhar essas informações com o usuário, de acordo com as políticas de gerenciamento de informações de sua organização. Para obter mais informações sobre essas ferramentas, consulte os links a seguir.

- AWS consultor de acesso — A ferramenta consultor de acesso AWS Identity and Access Management (IAM) permite determinar as permissões que seus desenvolvedores têm analisando o último registro de data e hora em que uma IAM entidade, como um usuário, função ou grupo, chamou um AWS serviço. É possível auditar o acesso ao serviço e remover as permissões desnecessárias, além de automatizar o processo, se necessário. Para obter mais informações, consulte nossa postagem no blog sobre AWS segurança.
- IAMsimulador de políticas — Com o simulador IAM de políticas, você pode testar e solucionar problemas de políticas baseadas em recursos e IAM baseadas em recursos. Para obter mais informações, consulte Testando IAM políticas com o simulador IAM de políticas.
- AWS CloudTrail registros — Você pode revisar AWS CloudTrail os registros para ver as ações realizadas por um usuário, função ou AWS service (Serviço da AWS). Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

  As ações tomadas pelos administradores da zona de pouso da AWS Control Tower podem ser visualizadas na conta de gerenciamento da zona de pouso. As ações tomadas pelos administradores e usuários da conta do membro podem ser visualizadas na conta de arquivamento de log compartilhado.

  Você pode ver uma tabela resumida dos eventos da AWS Control Tower na página Atividades.

## Explicando os controles preventivos

Um controle preventivo garante que as contas da sua organização mantenham a conformidade com suas políticas corporativas. O status de um controle preventivo é obrigatório ou não ativado. Um controle preventivo evita violações de políticas usando políticas de controle de serviço (SCPs). Em comparação, um controle de detetive informa sobre vários eventos ou estados que existem, por meio de regras definidas AWS Config .

Alguns de seus usuários, como AWS desenvolvedores, talvez precisem conhecer os controles preventivos que se aplicam a todas as contas que OUs eles usam, para que possam criar soluções

de engenharia. O procedimento a seguir oferece algumas orientações sobre como fornecer essas informações para os usuários certos, de acordo com as políticas de gerenciamento de informações da organização.

> **Note**
>
> Esse procedimento pressupõe que você já tenha criado pelo menos uma UO secundária em sua landing zone, bem como pelo menos um AWS IAM Identity Center usuário.

Para mostrar controles preventivos para usuários que precisam saber

1. Faça login no console do AWS Control Tower em https://console.aws.amazon.com/controltower/.
2. No painel de navegação à esquerda, escolha Organização.
3. Na tabela, escolha o nome de um dos OUs para os quais seu usuário precisa de informações sobre os controles aplicáveis.
4. Anote o nome da OU e os controles que se aplicam a essa OU.
5. Repita as duas etapas anteriores para cada UO sobre a qual o usuário precisa de informações.

Para obter informações detalhadas sobre os controles e suas funções, consulte Sobre os controles na AWS Control Tower.

## Planeje sua zona de pouso da AWS Control Tower

Quando você passa pelo processo de configuração, o AWS Control Tower inicia um recurso importante associado à sua conta, chamado landing zone, que serve como base para suas organizações e suas contas.

> **Note**
>
> É possível ter uma zona de destino por organização.

Para obter informações sobre algumas das melhores práticas a serem seguidas ao planejar e configurar sua landing zone, consulteAWS estratégia de várias contas para sua zona de pouso da AWS Control Tower.

Maneiras de configurar a AWS Control Tower

Você pode configurar uma zona de pouso da AWS Control Tower em uma organização existente ou pode começar criando uma nova organização que contenha sua zona de pouso da AWS Control Tower.

- Inicie AWS o Control Tower em uma organização existente: Esta seção é para clientes que já AWS Organizations estão prontos para serem governados pela AWS Control Tower.
- Lance a AWS Control Tower em uma nova organização: Esta seção é para clientes sem contas existentes AWS Organizations OUs, e.

> **Note**
>
> Se você já tem uma AWS Organizations landing zone, você pode estender a governança da AWS Control Tower da zona de pouso existente para algumas ou todas as suas contas existentes OUs e dentro de uma organização. Consulte Governar organizações e contas existentes.

## Compare a funcionalidade

Aqui está uma breve comparação das diferenças entre adicionar a AWS Control Tower a uma organização existente ou estender a governança da AWS Control Tower às OUs contas. Além disso, algumas considerações especiais se aplicam se você estiver migrando da solução AWS Landing Zone para a AWS Control Tower.

Sobre a adição a uma organização existente: Adicionar o AWS Control Tower a uma organização existente é algo que você pode fazer no AWS console. Nesse caso, você já criou uma organização no AWS Organizations serviço, essa organização não está atualmente registrada no AWS Control Tower e você deseja adicionar uma landing zone posteriormente.

Quando você adiciona uma landing zone a uma organização existente, a AWS Control Tower configura uma estrutura paralela, no AWS Organizations nível. Isso não altera as contas OUs e em sua organização existente.

Sobre a extensão da governança: A extensão da governança se aplica a contas específicas OUs dentro de uma única organização que já está registrada na AWS Control Tower, o que significa que já existe uma landing zone para essa organização. Estender a governança significa que os controles

da AWS Control Tower são estendidos para que suas restrições se apliquem às contas específicas OUs dessa organização registrada. Nesse caso, você não está lançando uma nova zona de pouso, está apenas expandindo a zona de pouso atual para sua organização.

> **Important**
>
> Consideração especial: Se você estiver usando atualmente a solução AWS Landing Zone (ALZ) para AWS Organizations, consulte seu arquiteto de AWS soluções antes de tentar habilitar o AWS Control Tower em sua organização. AWSA Control Tower não pode realizar verificações prévias que determinem se a AWS Control Tower pode interferir na implantação atual da sua landing zone. Para obter mais informações, consulte Passo a passo: mude do ALZ para o AWS Control Tower. Além disso, para obter informações sobre como mover contas de um landing zone para outra, consulte Se a conta não atender aos pré-requisitos

## Inicie AWS o Control Tower em uma organização existente

Ao configurar uma landing zone da AWS Control Tower em uma organização existente, você pode começar a trabalhar imediatamente, paralelamente ao seu AWS Organizations ambiente existente. Seus outros OUs criados dentro permanecem AWS Organizations inalterados, porque não estão registrados no AWS Control Tower. Você pode continuar a usá-las OUs e as contas exatamente como estão.

AWSO Control Tower se consolida usando a conta de gerenciamento de sua organização existente como sua conta de gerenciamento. Nenhuma nova conta de gerenciamento é necessária. Você pode iniciar sua zona de pouso do AWS Control Tower a partir da sua conta de gerenciamento existente.

> **Note**
>
> Para configurar o AWS Control Tower em uma organização existente, seus limites de serviço devem permitir a criação de pelo menos duas contas adicionais.

### Efeitos da adição da AWS Control Tower à sua organização existente

AWSA Control Tower cria duas contas em sua organização: uma conta de auditoria e uma conta de registro. Essas contas mantêm um registro das ações realizadas pela sua equipe, em suas contas individuais de usuário final. As contas de arquivamento de Auditoria e Registro aparecem na UO de Segurança dentro da landing zone da AWS Control Tower.

Quando você configura sua landing zone, as contas adicionadas pela AWS Control Tower se tornam parte de sua organização existente e AWS Organizations, como tal, tornam-se parte do faturamento de sua organização existente.

### Resumo das capacidades

Habilitar o AWS Control Tower em uma AWS Organizations organização existente fornece vários aprimoramentos importantes para a organização.

- Ele permite o faturamento unificado entre os grupos da sua organização, porque as contas adicionadas pelo AWS Control Tower se tornarão parte da sua organização existente.
- Ele permite que você administre todas as contas de uma conta de gerenciamento em sua OU.
- Ele simplifica a forma como você aplica e impõe controles que abrangem a segurança e a conformidade de contas novas e existentes.

> **Important**
>
> Lançar sua zona de pouso da AWS Control Tower em uma AWS Organizations organização existente não permite que você estenda a governança da AWS Control Tower dessa organização para outras OUs ou contas que não estejam registradas na AWS Control Tower.

Para iniciar o AWS Control Tower em sua organização existente, siga o processo descrito emComece a usar o AWS Control Tower.

Para obter mais informações sobre como a AWS Control Tower interage com AWS Organizations organizações existentes, consulteGoverne organizações e contas com a AWS Control Tower.

## Lance a AWS Control Tower em uma nova organização

Se você é novato na AWS Control Tower e ainda não trabalhou com ela AWS Organizations, o melhor lugar para começar é com nosso Configuração documento.

AWSA Control Tower configura uma organização para você automaticamente quando você não tem uma configurada.

# AWS estratégia de várias contas para sua zona de pouso da AWS Control Tower

AWSOs clientes da Control Tower geralmente buscam orientação sobre como configurar seu AWS ambiente e suas contas para obter melhores resultados.AWS criou um conjunto unificado de recomendações, chamado de estratégia de várias contas, para ajudar você a fazer o melhor uso de seus AWS recursos, incluindo sua landing zone da AWS Control Tower.

Essencialmente, o AWS Control Tower atua como uma camada de orquestração que funciona com outros AWS serviços, que ajudam você a implementar as recomendações de AWS várias contas para AWS contas e. AWS Organizations Depois que sua landing zone for configurada, a AWS Control Tower continuará ajudando você a manter suas políticas corporativas e práticas de segurança em várias contas e cargas de trabalho.

A maioria das zonas de pouso se desenvolve com o tempo. À medida que o número de unidades organizacionais (OUs) e contas na landing zone da AWS Control Tower aumenta, você pode estender a implantação da AWS Control Tower de forma a ajudar a organizar suas cargas de trabalho de forma eficaz. Este capítulo fornece orientação prescritiva sobre como planejar e configurar sua landing zone da AWS Control Tower, de acordo com a estratégia de AWS várias contas, e estendê-la ao longo do tempo.

Para uma discussão geral sobre as melhores práticas para unidades organizacionais, consulte Melhores práticas para unidades organizacionais com AWS Organizations.

## AWS estratégia de várias contas: orientação sobre as melhores práticas

AWS as melhores práticas para um ambiente bem arquitetado recomendam que você separe seus recursos e cargas de trabalho em várias contas. AWS Você pode pensar AWS nas contas como contêineres de recursos isolados: elas oferecem categorização da carga de trabalho, bem como redução do raio de explosão quando as coisas dão errado.

Definição de uma AWS conta

Uma AWS conta atua como um contêiner de recursos e um limite de isolamento de recursos.

> **Note**
>
> Uma AWS conta não é o mesmo que uma conta de usuário, que é configurada por meio de Federação ou AWS Identity and Access Management (IAM).

Mais sobre AWS contas

Uma AWS conta oferece a capacidade de isolar recursos e conter ameaças à segurança de suas AWS cargas de trabalho. Uma conta também fornece um mecanismo para cobrança e governança de um ambiente de carga de trabalho.

A AWS conta é o principal mecanismo de implementação para fornecer um contêiner de recursos para suas cargas de trabalho. Se seu ambiente for bem arquitetado, você poderá gerenciar várias AWS contas com eficiência e, assim, gerenciar várias cargas de trabalho e ambientes.

AWSA Control Tower configura um ambiente bem arquitetado. Além disso, ele depende de AWS contas que ajudam a controlar mudanças em seu ambiente que podem se estender a várias contas. AWS Organizations

Definição de um ambiente bem arquitetado

> AWS define um ambiente bem arquitetado como aquele que começa com uma landing zone.

AWSA Control Tower oferece uma landing zone que é configurada automaticamente. Ele impõe controles para garantir a conformidade com suas diretrizes corporativas em várias contas em seu ambiente.

Definição de landing zone

> O landing zone é um ambiente em nuvem que oferece um ponto de partida recomendado, incluindo contas padrão, estrutura de contas, layouts de rede e segurança, etc. A partir de uma landing zone, você pode implantar cargas de trabalho que utilizam suas soluções e aplicativos.

## Diretrizes para configurar um ambiente bem arquitetado

Os três componentes principais de um ambiente bem arquitetado, explicados nas seções a seguir, são:

- Várias AWS contas
- Várias unidades organizacionais (OUs)
- Uma estrutura bem planejada

### Use várias AWS contas

Uma conta não é suficiente para configurar um ambiente bem arquitetado. Ao usar várias contas, você pode oferecer melhor suporte às suas metas de segurança e processos comerciais. Aqui estão alguns benefícios de usar uma abordagem de várias contas:

- Controles de segurança — Os aplicativos têm perfis de segurança diferentes, portanto, exigem políticas e mecanismos de controle diferentes. Por exemplo, é muito mais fácil falar com um auditor e apontar para uma única conta que hospeda a carga de trabalho do setor de cartões de pagamento (PCI).
- Isolamento — Uma conta é uma unidade de proteção de segurança. Riscos potenciais e ameaças à segurança podem estar contidos em uma conta sem afetar outras pessoas. Portanto, as necessidades de segurança podem exigir que você isole as contas umas das outras. Por exemplo, você pode ter equipes com perfis de segurança diferentes.
- Muitas equipes — As equipes têm responsabilidades e necessidades de recursos diferentes. Ao configurar várias contas, as equipes não podem interferir umas nas outras, como fariam ao usar a mesma conta.
- Isolamento de dados — isolar os armazenamentos de dados em uma conta ajuda a limitar o número de pessoas que têm acesso aos dados e podem gerenciar o armazenamento de dados. Esse isolamento ajuda a evitar a exposição não autorizada de dados altamente privados. Por exemplo, o isolamento de dados ajuda a apoiar a conformidade com o Regulamento Geral de Proteção de Dados (GDPR).
- Processo de negócios — unidades de negócios ou produtos geralmente têm finalidades e processos completamente diferentes. Contas individuais podem ser estabelecidas para atender às necessidades específicas da empresa.
- Faturamento — Uma conta é a única maneira de separar itens em um nível de faturamento, incluindo itens como taxas de transferência e assim por diante. A estratégia de várias contas ajuda a criar itens faturáveis separados entre unidades de negócios, equipes funcionais ou usuários individuais.

- Alocação de cotas — as AWS cotas são configuradas por conta. A separação das cargas de trabalho em contas diferentes dá a cada conta (como um projeto) uma cota individual bem definida.

### Use várias unidades organizacionais

AWSA Control Tower e outras estruturas de orquestração de contas podem fazer alterações que ultrapassem os limites da conta. Portanto, as AWS melhores práticas tratam de mudanças em várias contas, que podem potencialmente prejudicar um ambiente ou prejudicar sua segurança. Em alguns casos, as mudanças podem afetar o ambiente geral, além das políticas. Como resultado, recomendamos que você configure pelo menos duas contas obrigatórias, Produção e Preparação.

Além disso, AWS as contas geralmente são agrupadas em unidades organizacionais (OUs), para fins de governança e controle. OUssão projetados para lidar com a aplicação de políticas em várias contas.

Nossa recomendação é que, no mínimo, você crie um ambiente de pré-produção (ou preparação) diferente do seu ambiente de produção, com controles e políticas distintos. Os ambientes de produção e preparação podem ser criados e administrados separadamente e faturados como contas separadasOUs. Além disso, talvez você queira configurar uma OU Sandbox para testes de código.

### Use uma estrutura bem planejada para OUs sua landing zone

AWSA Control Tower configura alguns OUs para você automaticamente. À medida que suas cargas de trabalho e requisitos se expandem com o tempo, você pode estender a configuração original do landing zone para atender às suas necessidades.

> **Note**
>
> Os nomes fornecidos nos exemplos seguem as convenções de AWS nomenclatura sugeridas para configurar um ambiente com várias AWS contas. Você pode renomear sua OUs depois de configurar sua landing zone, selecionando Editar na página de detalhes da OU.

### Recomendações

Depois que a AWS Control Tower configurar a primeira OU necessária para você — a OU de segurança —, recomendamos criar alguma unidade adicional OUs em sua landing zone.

Recomendamos que você permita que o AWS Control Tower crie pelo menos uma OU adicional, chamada Sandbox OU. Essa OU é para seus ambientes de desenvolvimento de software. AWSA Control Tower pode configurar a OU Sandbox para você durante a criação da landing zone, se você a selecionar.

Duas outras recomendadas OUs que você pode configurar por conta própria: a UO de Infraestrutura, para conter seus serviços compartilhados e contas de rede, e uma OU para conter suas cargas de trabalho de produção, chamada de UO de Cargas de Trabalho. Você pode adicionar mais OUs em sua landing zone por meio do console AWS Control Tower na página de unidades organizacionais.

Recomendado, OUs além dos configurados automaticamente

- Infraestrutura OU — contém seus serviços compartilhados e contas de rede.

> **Note**
>
> AWSA Control Tower não configura a UO de infraestrutura para você.

- Sandbox OU — Uma OU de desenvolvimento de software. Por exemplo, ele pode ter um limite fixo de gastos ou pode não estar conectado à rede de produção.

> **Note**
>
> AWSA Control Tower recomenda que você configure a Sandbox OU, mas ela é opcional. Ele pode ser configurado automaticamente como parte da configuração da sua landing zone.

- Cargas de trabalho OU — contém contas que executam suas cargas de trabalho.

> **Note**
>
> AWSA Control Tower não configura a OU de cargas de trabalho para você.

Para obter mais informações, consulte Organização inicial de produção com AWS Control Tower.

# Exemplo de AWS Control Tower com uma estrutura completa de OU para várias contas

AWSO Control Tower suporta uma hierarquia de OU aninhada, o que significa que você pode criar uma estrutura hierárquica de OU que atenda aos requisitos da sua organização. Você pode criar um ambiente AWS Control Tower de acordo com a orientação estratégica de AWS várias contas.

Você também pode criar uma estrutura de OU mais simples e plana que tenha um bom desempenho e esteja alinhada com a orientação de AWS várias contas. Só porque você pode criar uma estrutura hierárquica de OU, isso não significa que você deva fazer isso.

- Para ver um diagrama que mostra um conjunto de exemplos OUs em um ambiente expandido e plano de AWS Control Tower com orientação para AWS várias contas, consulte Exemplo: cargas de trabalho em uma estrutura de OU plana.
- Para obter mais informações sobre como a AWS Control Tower funciona com estruturas de OU aninhadas, consulteOUs aninhadas na AWS Control Tower.
- Para obter mais informações sobre como a AWS Control Tower se alinha à AWS orientação, consulte o AWS white paper Organizing Your AWS Environment Using Multiple Accounts.

O diagrama na página vinculada mostra que mais Fundamentais OUs e mais Adicionais OUs foram criados. Eles OUs atendem às necessidades adicionais de uma implantação maior.

Na OUs coluna Fundamental, duas OUs foram adicionadas à estrutura básica:

- Security_Prod OU — Fornece uma área somente de leitura para políticas de segurança, bem como uma área de auditoria de segurança incomparável.
- UO de infraestrutura — Talvez você queira separar a OU de infraestrutura, recomendada anteriormente, em duasOUs, Infrastructure_Test (para infraestrutura de pré-produção) e Infrastructure_Prod (para infraestrutura de produção).

Na OUs área adicional, várias outras OUs foram adicionadas à estrutura básica. Estes são os próximos itens recomendados OUs para criar à medida que seu ambiente cresce:

- UO de cargas de trabalho — A OU de cargas de trabalho, recomendada anteriormente, mas opcional, foi separada em duasOUs, Workloads_Test (para cargas de trabalho de pré-produção) e Workloads_Prod (para cargas de trabalho de produção).

- PolicyStaging OU — Permite que os administradores do sistema testem suas alterações nos controles e políticas antes de aplicá-las totalmente.
- OU suspensa — Oferece um local para contas que podem ter sido desativadas temporariamente.

### Sobre o Root

A raiz não é uma OU. É um contêiner para a conta de gerenciamento e para todas as OUs contas da sua organização. Conceitualmente, a raiz contém todos os. OUs Ele não pode ser excluído. Você não pode controlar contas inscritas no nível Raiz dentro da AWS Control Tower. Em vez disso, controle as contas inscritas em seu. OUs Para obter um diagrama útil, consulte a AWS Organizations documentação.

## Dicas administrativas para configuração da landing zone

Aqui estão algumas dicas para configurar sua landing zone.

- A AWS região onde você trabalha mais deve ser sua região de origem.
- Configure sua landing zone e implante suas contas Account Factory de dentro da sua região natal.
- Se você estiver investindo em várias AWS regiões, certifique-se de que seus recursos de nuvem estejam na região em que você fará a maior parte do trabalho administrativo da nuvem e executará suas cargas de trabalho.
- Ao manter suas cargas de trabalho e registros na mesma AWS região, você reduz o custo associado à movimentação e recuperação de informações de registro entre regiões.
- A auditoria e outros buckets do Amazon S3 são criados na mesma AWS região a partir da qual você executa o Control TowerAWS. Recomendamos que você não mova esses buckets.
- Você pode criar seus próprios buckets de log na conta do Log Archive, mas isso não é recomendado. Certifique-se de deixar os buckets criados pela AWS Control Tower.
- Seus logs de acesso ao Amazon S3 devem estar na mesma AWS região dos buckets de origem.
- Ao iniciar, os endpoints do AWS Security Token Service (STS) devem ser ativados na conta de gerenciamento para todas as regiões suportadas pelo AWS Control Tower. Caso contrário, a execução pode falhar no meio do processo de configuração.
- AWSO Control Tower suporta marcação somente para controles ativados. Para obter mais informações, consulte AWSO Control Tower suporta marcação para controles habilitados.
- Recomendamos ativar a autenticação multifator (MFA) para cada conta gerenciada pela AWS Control Tower.

Considerações sobre VPCs

- O VPC criado pela AWS Control Tower é limitado àqueles Regiões da AWS em que o AWS Control Tower está disponível. Alguns clientes cujas cargas de trabalho são executadas em regiões não suportadas podem querer desativar o VPC que é criado com sua conta Account Factory. Eles podem preferir criar um novo VPC usando o portfólio do Service Catalog ou criar um personalizado VPC que seja executado somente nas regiões necessárias.
- O VPC criado pelo AWS Control Tower não é o mesmo VPC que o padrão criado para todos Contas da AWS. Nas regiões em que a AWS Control Tower é suportada, a AWS Control Tower exclui o padrão VPC ao criar a AWS Control TowerVPC.
- Se você excluir seu padrão VPC em sua AWS região de origem, é melhor excluí-lo em todas as outras AWS regiões.

# Recomendações para configurar grupos, funções e políticas

Conforme você configura sua zona de destino, é recomendável decidir antecipadamente quais usuários precisarão acessar determinadas contas e por quê. Por exemplo, uma conta de segurança deve estar acessível somente para a equipe de segurança, a conta de gerenciamento deve estar acessível somente para a equipe de administradores de nuvem e assim por diante.

Para obter mais informações sobre esse tópico, consulteGerenciamento de identidade e acesso na AWS Control Tower.

Restrições recomendadas

Você pode restringir o escopo do acesso administrativo às suas organizações configurando uma IAM função ou política que permita aos administradores gerenciar somente as ações da AWS Control Tower. A abordagem recomendada é usar a IAM políticaarn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy. Com a AWSControlTowerServiceRolePolicy função ativada, um administrador pode gerenciar somente o AWS Control Tower. Certifique-se de incluir acesso adequado AWS Organizations para gerenciar seus controles preventivos e acesso a SCPs AWS Config, para gerenciar controles de detetive, em cada conta.

Ao configurar a conta de auditoria compartilhada em sua zona de destino, recomendamos a atribuição do grupo AWSSecurityAuditors a quaisquer auditores externos de suas contas. Esse grupo concede permissão somente leitura a seus membros. Uma conta não deve ter permissões de

gravação no ambiente em que está realizando auditoria, pois pode violar a conformidade com os requisitos de separação de funções para auditores.

Você pode impor condições nas políticas de confiança de sua função para restringir as contas e os recursos que interagem com determinadas funções na AWS Control Tower. É altamente recomendável que você restrinja o acesso à `AWSControlTowerAdmin` função, pois ela permite amplas permissões de acesso. Para obter mais informações, consulte Condições opcionais para as relações de confiança da sua função.

## Orientação para criar e modificar recursos da AWS Control Tower

Recomendamos as seguintes melhores práticas ao criar e modificar recursos na AWS Control Tower. Esta orientação pode mudar à medida que o serviço é atualizado. Lembre-se de que o modelo de responsabilidade compartilhada se aplica ao seu ambiente AWS Control Tower.

Orientação geral

- Não modifique nem exclua nenhum recurso criado pela AWS Control Tower, incluindo recursos na conta de gerenciamento, nas contas compartilhadas e nas contas dos membros. Se você modificar esses recursos, talvez seja necessário atualizar sua landing zone ou registrar novamente uma OU, e a modificação pode resultar em relatórios de conformidade imprecisos.

  Em particular:

  - Mantenha um AWS Config gravador ativo. Se você excluir seu gravador Config, os controles de detetive não poderão detectar e relatar desvios. Recursos não compatíveis podem ser relatados como compatíveis devido à insuficiência de informações.
  - Não modifique nem exclua as funções AWS Identity and Access Management (IAM) criadas nas contas compartilhadas na unidade organizacional (OU) de segurança. A modificação dessas funções pode exigir uma atualização da sua zona de destino.
  - Não exclua a `AWSControlTowerExecution` função de suas contas de membros, mesmo em contas não inscritas. Se você fizer isso, não poderá cadastrar essas contas no AWS Control Tower nem registrar seus pais OUs imediatos.
- Não proíba o uso de nenhum Regiões da AWS por meio de SCPs ou AWS Security Token Service (AWS STS). Isso fará com que o AWS Control Tower entre em um estado indefinido. Se você proibir regiões com AWS STS, sua funcionalidade falhará nessas regiões, porque a autenticação não estaria disponível nessas regiões. Em vez disso, confie na AWS capacidade de negar a região da Control Tower, conforme mostrado no controle, Negar acesso AWS com base no solicitado

Região da AWS, que funciona no nível da zona de pouso, ou no controle de negação da região de controle aplicado à OU, que funciona no nível da OU para restringir o acesso às regiões.

- O AWS Organizations `FullAWSAccess` SCP deve ser aplicado e não deve ser mesclado com outroSCPs. Alterar isso não SCP é relatado como desvio; no entanto, algumas mudanças podem afetar a funcionalidade do AWS Control Tower de maneiras imprevisíveis, se o acesso a determinados recursos for negado. Por exemplo, se SCP for desanexada ou modificada, uma conta poderá perder o acesso a um AWS Config gravador ou criar uma lacuna no CloudTrail registro.
- Não use o AWS Organizations `DisableAWSServiceAccess` API para desativar o acesso do serviço AWS Control Tower à organização em que você configurou sua landing zone. Se você fizer isso, alguns recursos de detecção de desvio do AWS Control Tower podem não funcionar corretamente sem o suporte de mensagens do AWS Organizations. Esses recursos de detecção de desvios ajudam a garantir que a AWS Control Tower possa relatar o status de conformidade de unidades organizacionais, contas e controles em sua organização com precisão. Para ter mais informações, consulte API_DisableAWSServiceAccess na AWS Organizations Referência da API.
- Em geral, o AWS Control Tower executa uma única ação por vez, que deve ser concluída antes que outra ação possa começar. Por exemplo, se você tentar provisionar uma conta enquanto o processo de habilitação de um controle já estiver em operação, o provisionamento da conta falhará.

  Exceção:

  - AWSO Control Tower permite ações simultâneas para implantar controles opcionais. Para obter mais informações, consulte Implantação simultânea para controles opcionais.
  - AWSO Control Tower permite até dez ações simultâneas de criação, atualização ou inscrição em contas, com o Account Factory.

> **Note**
>
> Para obter mais informações sobre os recursos criados pelo AWS Control Tower, consulteQuais são as contas compartilhadas?.

Dicas sobre contas e OUs

- Recomendamos que você mantenha cada OU registrada em um máximo de 1.000 contas, para que você possa atualizar essas contas com o recurso Registrar novamente a OU sempre que forem necessárias atualizações de conta, como ao configurar novas regiões para governança.
- Para reduzir o tempo necessário ao registrar uma OU, recomendamos que você mantenha o número de contas por OU em torno de 680, mesmo que o limite seja de 1.000 contas por OU. Como regra geral, o tempo necessário para registrar uma OU aumenta de acordo com o número de regiões nas quais sua OU está operando, multiplicado pelo número de contas na OU.
- Como estimativa, uma OU com 680 contas pode exigir até 2 horas para se registrar e ativar os controles, e até 1 hora para se registrar novamente. Além disso, uma OU que tem muitos controles leva mais tempo para ser registrada do que uma OU com poucos controles.
- Uma preocupação em permitir um prazo maior para registrar uma OU é que esse processo bloqueia outras ações. Alguns clientes se sentem confortáveis em permitir períodos mais longos para registrar ou registrar novamente uma OU, porque preferem permitir mais contas em cada OU.

# Quando fazer login como usuário root

Determinadas tarefas administrativas exigem que você faça login como usuário raiz. Você pode entrar como usuário root em um Conta da AWS que foi criado pela fábrica de contas na AWS Control Tower.

É necessário fazer login como usuário raiz para executar as seguintes ações:

- Alterar determinadas configurações da conta, incluindo o nome da conta, a senha do usuário raiz ou o endereço de e-mail. Para obter mais informações, consulte Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog.
- Para fechar um Conta da AWS.
- Para obter mais informações sobre ações que exigem credenciais de login do usuário raiz, consulte Tarefas que exigem credenciais do usuário raiz no Guia de AWS Account Management referência.

> **Note**
>
> Para alterar ou ativar seu plano do AWS Support, você deve estar conectado como usuário root ou ser um usuário com as IAM permissões apropriadas. .

Para fazer login como usuário raiz

1. Abra a página AWS de login.

   Se você não tiver o endereço de e-mail Conta da AWS ao qual precisa acessar, você pode obtê-lo na AWS Control Tower. Abra o console da conta de gerenciamento, escolha Contas e procure o endereço de e-mail.
2. Insira o endereço de e-mail do Conta da AWS ao qual você precisa acessar e escolha Avançar.
3. Escolha Forgot password? (Esqueceu a senha?) para receber instruções de redefinição de senha no endereço de e-mail do usuário raiz.
4. Abra a mensagem do e-mail de redefinição de senha da caixa de e-mails do usuário raiz e siga as instruções para redefinir a sua senha.
5. Abra a página de AWS login e, em seguida, faça login com sua senha redefinida.

# AWS Organizations orientação

AWSA Control Tower está intimamente associada AWS Organizations a. Aqui estão algumas orientações específicas sobre como elas funcionam melhor juntas para proteger seu AWS meio ambiente.

- Você pode encontrar orientações sobre as melhores práticas para proteger a segurança da sua conta de gerenciamento da AWS Control Tower e das contas dos membros na AWS Organizations documentação.
  - Melhores práticas para a conta de gerenciamento
  - Melhores práticas para contas de membros
- Não use AWS Organizations para atualizar políticas de controle de serviço (SCPs) anexadas a uma OU registrada na AWS Control Tower. Isso pode fazer com que os controles entrem em um estado desconhecido, o que exigirá que você redefina sua landing zone ou registre novamente sua OU na AWS Control Tower. Em vez disso, você pode criar novos SCPs e anexá-los ao OUs invés de editar o SCPs que a AWS Control Tower criou.

- Mover contas individuais, já inscritas, para o AWS Control Tower, de fora de uma OU registrada, causa um desvio que deve ser resolvido. Consulte Tipos de oscilação de governança.
- Se você usa AWS Organizations para criar, convidar ou mover contas dentro de uma organização registrada na AWS Control Tower, essas contas não são inscritas pela AWS Control Tower e essas alterações não são registradas. Se você precisar acessar essas contas por meio deSSO, consulte Acesso à conta de membro.
- Se você usa AWS Organizations para mover uma OU para uma organização criada pela AWS Control Tower, a OU externa não é registrada pela AWS Control Tower.
- AWSA Control Tower lida com a filtragem de permissões de forma diferente AWS Organizations . Se suas contas forem provisionadas com a fábrica de contas da AWS Control Tower, os usuários finais poderão ver os nomes e os pais de todas OUs no console da AWS Control Tower, mesmo que não tenham permissão para recuperar esses nomes e pais diretamente. AWS Organizations
- AWSO Control Tower não oferece suporte a permissões mistas em organizações, como permissão para visualizar o pai de uma OU, mas não para ver os nomes de UO. Por esse motivo, espera-se que os administradores da AWS Control Tower tenham permissões completas.
- O AWS Organizations `FullAWSAccess` SCP deve ser aplicado e não deve ser mesclado com outroSCPs. Alterar isso não SCP é relatado como desvio; no entanto, algumas mudanças podem afetar a funcionalidade do AWS Control Tower de maneiras imprevisíveis, se o acesso a determinados recursos for negado. Por exemplo, se SCP for desanexada ou modificada, uma conta poderá perder o acesso a um AWS Config gravador ou criar uma lacuna no CloudTrail registro.
- Não use o AWS Organizations `DisableAWSServiceAccess` API para desativar o acesso do serviço AWS Control Tower à organização em que você configurou sua landing zone. Se você fizer isso, alguns recursos de detecção de desvio do AWS Control Tower podem não funcionar corretamente sem o suporte de mensagens do AWS Organizations. Esses recursos de detecção de desvios ajudam a garantir que a AWS Control Tower possa relatar o status de conformidade de unidades organizacionais, contas e controles em sua organização com precisão. Para ter mais informações, consulte API_DisableAWSServiceAccess na AWS Organizations Referência da API.

# IAMOrientação do Identity Center

AWSA Control Tower recomenda que você use AWS Identity and Access Management (IAM) para regular o acesso ao seu Contas da AWS. No entanto, você tem a opção de escolher se o AWS Control Tower configura o IAM Identity Center para você, se você configura o IAM Identity Center

para você mesmo, de uma forma que atenda às suas necessidades comerciais com mais eficiência, ou se deseja selecionar outro método para acessar a conta.

> **Note**
>
> SSOé uma abreviatura usada no setor de tecnologia para indicar login único. Em termos gerais, SSO é um serviço de autenticação de sessão e usuário. Ele permite que alguém use um conjunto de credenciais de login para acessar vários aplicativos. Ao nos referirmos ao recurso de login único em AWS, estamos nos referindo ao AWS serviço chamado AWS Identity and Access Managemente abreviado como IAMIdentity Center. IAM

Por padrão, o AWS Control Tower configura o AWS IAM Identity Center para sua landing zone, de acordo com as diretrizes de melhores práticas definidas em Organizando seu AWS ambiente usando várias contas. A maioria dos clientes escolhe o padrão. Às vezes, métodos alternativos de acesso são necessários para conformidade regulatória em setores ou países específicos ou Regiões da AWS onde o AWS IAM Identity Center não está disponível.

Escolhendo uma opção

No console, você pode optar por autogerenciar o IAM Identity Center durante o processo de configuração da landing zone, em vez de permitir que a AWS Control Tower o configure para você. A qualquer momento, você pode optar por alterar essa seleção, modificando as configurações da zona de pouso e atualizando sua zona de pouso na página de configurações da zona de pouso.

Para descontinuar o AWS IAM Identity Center no AWS Control Tower ou para começar a usar o AWS IAM Identity Center

1. Navegue até a página de configurações do landing zone
2. Selecione a guia Configurações
3. Em seguida, escolha o botão de rádio apropriado para alterar sua seleção para o AWS IAM Identity Center.

Depois de optar por autogerenciar o AWS IAM Identity Center como seu IdPAWS, o Control Tower cria somente as funções e políticas necessárias para gerenciar a Control AWS Tower, como e. `AWSControlTowerAdmin` `AWSControlTowerAdminPolicy` Para zonas de pouso que se autogerenciam, a AWS Control Tower não cria mais IAM funções e agrupamentos para uso

específico do cliente, nem durante o processo de configuração da zona de pouso, nem durante o provisionamento da conta com o Account Factory.

> **Note**
>
> Se você remover o AWS IAM Identity Center da sua landing zone da AWS Control Tower, os usuários, grupos e conjuntos de permissões criados pela AWS Control Tower não serão removidos. Recomendamos que você remova esses recursos.

Clientes do Account Factory com provedores de identidade alternativos (IdPs), como Azure AD, Ping ou Okta, podem seguir o processo do AWS IAM Identity Center para se conectar a um provedor de identidade externo e integrar seu IdP. Você pode voltar a fazer com que o AWS Control Tower gere seus agrupamentos e funções a qualquer momento, modificando as configurações da landing zone.

- Para obter informações específicas sobre como o AWS Control Tower funciona com o IAM Identity Center com base em sua fonte de identidade, consulte Considerações para AWS IAM Identity Center clientes na seção Verificações de pré-lançamento da página de introdução deste Guia do usuário.
- Para obter informações adicionais sobre como o comportamento do AWS Control Tower interage com o IAM Identity Center e com diferentes fontes de identidade, consulte Considerações para alterar sua fonte de identidade no Guia do usuário do IAM Identity Center.
- Consulte Trabalhando com o AWS IAM Identity Center e o AWS Control Tower para obter mais informações sobre como trabalhar com o AWS Control Tower e o IAM Identity Center.

## Orientação do Account Factory

Você pode encontrar problemas ao usar o Account Factory para provisionar uma nova conta na AWS Control Tower. Para obter informações sobre como solucionar esses problemas, consulte a seção Falha no provisionamento de novas contas Solução de problemas do Guia do Usuário do AWS Control Tower.

Recomendamos que você crie usuários ou IAM funções federados em vez de IAM usuários. Usuários e IAM funções federados fornecem credenciais temporárias. IAMos usuários têm credenciais de longo prazo que podem ser difíceis de gerenciar. Para obter mais informações, consulte IAMidentidades (usuários, grupos de usuários e funções) no Guia do IAM usuário.

Se você estiver autenticado como IAM usuário ou usuário do IAM Identity Center ao provisionar uma nova conta no Account Factory ou ao usar o recurso de inscrição de conta Control TowerAWS, verifique se o usuário tem acesso ao seu portfólio. AWS Service Catalog Caso contrário, você poderá receber uma mensagem de erro do Service Catalog. Para obter mais informações, consulte a Nenhum erro de caminhos de inicialização encontrado seção Solução de problemas do Guia do Usuário do AWS Control Tower.

> **Note**
>
> Até cinco contas podem ser provisionadas por vez.

## Orientação sobre como se inscrever em Tópicos SNS

Inscreva-se nos SNS tópicos para obter informações sobre seu ambiente AWS Control Tower.

- O `aws-controltower-AllConfigNotifications` SNS tópico recebe todos os eventos publicados pela AWS Config, incluindo notificações de conformidade e notificações de CloudWatch eventos da Amazon. Por exemplo, este tópico informa se ocorreu uma violação de controle. Também fornece informações sobre outros tipos de eventos. (Saiba mais AWS Configsobre o que eles publicam quando esse tópico é configurado.)
- Os eventos de dados da `aws-controltower-BaselineCloudTrail` trilha também estão configurados para serem publicados no `aws-controltower-AllConfigNotifications` SNS tópico.
- Para receber notificações detalhadas de conformidade, recomendamos que você assine o `aws-controltower-AllConfigNotifications` SNS tópico. Este tópico agrega notificações de conformidade de todas as contas secundárias.
- Para receber notificações de deriva e outras notificações, bem como notificações de conformidade, mas menos notificações em geral, recomendamos que você se inscreva no `aws-controltower-AggregateSecurityNotifications` SNS tópico.
- Para receber notificações sobre erros do AWS Control Tower Account Factory for Terraform (AFT), você pode se inscrever em um SNS tópico chamado aft_failure_notifications, exibido no AFT repositório. Por exemplo:

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
```

```
}
```

- Todos os SNS tópicos são criptografados em repouso com criptografia de disco. Para obter mais informações, consulte Criptografia de dados.

Para obter mais informações sobre SNS tópicos e conformidade, consulte Prevenção e notificação.

## Orientação para KMS chaves

AWSO Control Tower funciona com AWS Key Management Service (AWS KMS). Opcionalmente, se você quiser criptografar e descriptografar seus recursos da Control AWS Tower com uma chave de criptografia gerenciada por você, você pode gerar e configurar. AWS KMS keys Você pode adicionar ou alterar uma KMS chave sempre que atualizar sua landing zone. Como prática recomendada, recomendamos usar suas próprias KMS chaves e alterá-las de tempos em tempos.

AWS KMS permite criar chaves multirregionais e KMS chaves assimétricas. No entanto, AWS o Control Tower não oferece suporte a teclas multirregionais ou assimétricas. AWSO Control Tower executa uma pré-verificação das chaves existentes. Você pode ver uma mensagem de erro se selecionar uma chave multirregional ou uma chave assimétrica. Nesse caso, gere outra chave para uso com os recursos da AWS Control Tower.

Para clientes que operam um HSM cluster de AWS nuvem: crie um armazenamento de chaves personalizado associado ao seu HSM cluster de nuvem. Em seguida, você pode criar uma KMS chave, que reside no armazenamento de chaves HSM personalizadas do Cloud que você criou. Você pode adicionar essa KMS chave à AWS Control Tower.

Você deve fazer uma atualização específica na política de permissões de uma KMS chave para que ela funcione com a AWS Control Tower. Para obter detalhes, consulte a seção chamadaAtualize a política de KMS chaves.

## Práticas recomendadas para atualizações da landing zone

Esta seção fornece algumas considerações e melhores práticas que você deve ter em mente ao considerar uma atualização da sua versão de landing zone no AWS Control Tower. A mudança da série 2.0 da versão da zona de pouso para a série da versão 3.0 da zona de pouso é especialmente importante. Quando você atualiza sua landing zone, o AWS Control Tower automaticamente move você para a versão mais recente disponível.

> **Note**
>
> É uma prática recomendada atualizar para a versão mais recente da landing zone.

Resumo das melhores práticas explicadas nesta seção

- Prática recomendada: por motivos de segurança e auditoria, é altamente recomendável que você ative o registro geral, para todas as contas, e envie as informações de registro para um local centralizado. No AWS Control Tower, esse local centralizado é a conta de arquivamento de registros, que fornece um bucket de registro do Amazon S3.
- Melhor prática: se você optar por não participar da CloudTrail trilha de nível organizacional no AWS Control Tower, configure e gerencie suas próprias trilhas.
- Prática recomendada: ao operar seu ambiente AWS Control Tower, configure um ambiente de teste.

Benefícios de mudar das versões 2.x da zona de pouso para as versões 3.x da zona de pouso

- Registre AWS Config recursos somente na região de origem, o que gera economia de custos ao gerenciar recursos globais
- Criptografe sua AWS CloudTrail trilha com sua própria chave KMS
- Personalize seu cronograma de retenção de registros
- Controles obrigatórios aprimorados
- Maior número de controles disponíveis
- Integrado com AWS Security Hub
- Atualizações de tempo de execução do Python

Advertências para mudar das versões 2.x da zona de pouso para as versões 3.x da zona de pouso

- Com o landing zone 3.0 e versões posteriores, o AWS Control Tower não suporta mais AWS CloudTrail trilhas gerenciadas em nível de conta. AWS
- Você tem a opção de escolher uma trilha de nível organizacional gerenciada pela AWS Control Tower ou optar por não participar e gerenciar suas próprias trilhas. CloudTrail

- Existe a possibilidade de custos duplos, especialmente se algumas contas em uma OU não estiverem inscritas na AWS Control Tower e tiverem suas próprias trilhas em nível de conta que você deseja manter.

### Considerações sobre a escolha de trilhas em nível organizacional CloudTrail

- Quando você atualiza para 3.0 ou posterior, o AWS Control Tower exclui as trilhas no nível da conta que ele criou originalmente, após 24 horas.
- Nenhum dado dessas trilhas é perdido. Seus registros existentes são preservados mesmo quando as trilhas são removidas.
- AWSA Control Tower cria um novo caminho no mesmo bucket do Amazon S3 para as trilhas, para diferenciar as trilhas no nível da conta das trilhas no nível da organização.
  - O caminho do registro de trilhas da conta tem o seguinte formato: `/orgId/AWSLogs/...`
  - O caminho do registro de trilhas da organização tem o seguinte formato: `/orgId/AWSLogs/orgId/...`
- CloudTrail Trilhas adicionais que você implantou, trilhas não implantadas pela AWS Control Tower, não são tocadas.
- Todas as contas são incluídas na trilha em nível de organização, incluindo contas não inscritas na Torre de AWS Controle, se as contas não inscritas fizerem parte de uma OU registrada.
- Os CloudWatch alarmes da Amazon em contas vinculadas não são acionados.
- Se você optar por não participar de uma trilha em nível organizacional, a AWS Control Tower ainda criará a trilha, mas definirá seu status como Desativado.
- Como prática recomendada, se você optar por não participar da trilha em nível organizacional no AWS Control Tower, deverá configurar e gerenciar suas próprias trilhas, CloudTrail

### Benefícios das trilhas em nível organizacional

- A trilha da organização funciona em todas as contas na OU.
- Os itens registrados são padronizados e não podem ser modificados pelos usuários da conta.

### Considere um ambiente de teste

Quando você atualiza sua landing zone, o AWS Control Tower faz alterações somente nas contas compartilhadas e na OU Foundational. Ele não faz alterações em suas contas de carga de trabalho ouOUs. No entanto, como prática recomendada, ao operar seu ambiente AWS Control Tower,

recomendamos que você configure um ambiente de teste. Dentro do ambiente de teste isolado, você pode testar as atualizações da zona de pouso do AWS Control Tower, bem como quaisquer alterações que você possa fazer nas políticas de controle de serviço (SCPs), e você pode testar os controles que deseja aplicar ao ambiente. Essa recomendação é especialmente útil se você estiver operando em um setor regulamentado,

## Serviços baseados em IA e AWS Control Tower

Você pode criar políticas de controle de serviço (SCPs) que permitem que você opte por não ter seus dados armazenados por serviços baseados AWS em IA ativados. Essas SCP políticas especificam que serviços baseados em IA, como Amazon Rekognition ou CodeWhisperer Amazon, não podem armazenar e usar seus dados para melhorar outros serviços baseados em IA. AWS

Essas SCP políticas de exclusão de IA podem ser aplicadas a toda a sua organização, a uma OU ou a uma conta específica. As políticas têm efeito global. Você pode encontrar mais informações sobre essas políticas em Políticas de exclusão de serviços de IA, na AWS Organizations documentação.

Para obter uma lista de AWS serviços que usam IA, junto com exemplos de políticas, consulte a sintaxe e exemplos de políticas de exclusão de serviços de IA no Guia do AWS Organizations usuário.

# Gerenciamento de atualizações de configuração no AWS Control Tower

É responsabilidade dos membros da sua equipe central de administradores de nuvem manter sua landing zone atualizada. Atualizar sua landing zone garante que a AWS Control Tower seja corrigida e atualizada. Além disso, para proteger sua landing zone de possíveis problemas de conformidade, os membros da equipe central de administradores de nuvem devem resolver os problemas de deriva assim que forem detectados e relatados.

> **Note**
>
> O console AWS Control Tower indica quando sua landing zone precisa ser atualizada. Se você não vê uma opção de atualização, sua landing zone já está atualizada.

A tabela a seguir contém uma lista das versões de atualização da zona de pouso do AWS Control Tower, com links para as descrições de cada versão.

| Version (Versão) | Data de lançamento | Descrição |
|---|---|---|
| 3.3 | 12-12-2023 | Zona de pouso versão 3.3 |
| 3.2 | 6-09-2023 | Zona de pouso versão 3.2 |
| 3.1 | 2-09-2023 | Zona de pouso versão 3.1 |
| 3.0 | 26/07/2022 | Zona de pouso versão 3.0 |
| 2.9 | 22/04/2022 | Zona de pouso versão 2.9 |
| 2.8 | 2-10-2022 | Zona de pouso versão 2.8 |
| 2.7 | 4-8-2021 | Zona de pouso versão 2.7 |
| 2.6 | 29/12/2020 | Zona de pouso versão 2.6 |
| 2,5 | 11-18-2020 | Zona de pouso versão 2.5 |

| Version (Versão) | Data de lançamento | Descrição |
| --- | --- | --- |
| 2.4 | Nenhum | Nenhum |
| 2.3 | 3-5-2020 | Zona de pouso versão 2.3 |
| 2.2 | 11-13-19 | Zona de pouso versão 2.2 |
| 2.1 | 6-24-19 | Zona de pouso versão 2.1 |

Cada vez que você atualiza sua zona de pouso, você tem a oportunidade de modificar as configurações da sua zona de pouso.

Benefícios da atualização

- Você pode alterar suas regiões governadas
- Você pode alterar sua política de retenção de registros
- Você pode adicionar ou remover o controle de negação de região
- Você pode aplicar chaves AWS KMS de criptografia
- Você pode ativar ou desativar sua trilha no nível da organização CloudTrail .
- Você pode resolver o desvio da landing zone

Ao atualizar sua landing zone, você recebe automaticamente os recursos mais recentes do AWS Control Tower. Veja a versão atual da sua zona de pouso na página de configurações da zona de pouso.

Se uma atualização falhar, o AWS Control Tower não voltará para uma versão anterior da landing zone. Você pode encontrar seu landing zone em um estado indeterminado. Em caso afirmativo, entre em contato com AWS o suporte. Para obter mais informações sobre como solucionar uma falha na atualização, consulteNão é possível atualizar a zona de aterrissagem.

Você tem a oportunidade de limpar mapeamentos não utilizados do AWS Identity Center (anteriormente chamado AWS SSO) ao atualizar sua landing zone. Para obter mais informações, consulte Notas de campo: limpar mapeamentos não utilizados do IAM Identity Center automaticamente durante as atualizações da AWS Control Tower.

Pré-requisito para atualização e redefinição — desative o Requester Pays

Antes de atualizar ou redefinir sua landing zone, certifique-se de que o bucket de registro do Amazon S3 para a conta do Log Archive não tenha o recurso Requester Pays ativado. Você deve desativar esse recurso antes de iniciar o processo de atualização ou redefinição. Quando a AWS Control Tower configura seu bucket de registro, esse recurso não é ativado. Portanto, somente os clientes que ativaram posteriormente o recurso Requester Pays devem desativá-lo. Para obter mais informações, consulte a política de bucket do Amazon S3 para CloudTrail e o uso de buckets do Requester Pays.

## Sobre as atualizações da landing zone

As atualizações são necessárias para corrigir a mudança de governança ou para migrar para uma nova versão do AWS Control Tower. Para realizar uma atualização completa do AWS Control Tower, você deve primeiro atualizar sua landing zone e depois atualizar as contas inscritas individualmente. Talvez seja necessário executar três tipos de atualizações em momentos diferentes.

- Uma atualização da zona de pouso: na maioria das vezes, esse tipo de atualização é realizado escolhendo Atualizar na página de configurações da zona de pouso. Talvez seja necessário realizar uma atualização da landing zone para resolver certos tipos de deriva, e você pode escolher Redefinir quando necessário.
- Uma atualização de uma ou mais contas individuais: será necessário atualizar contas se as informações associadas forem alteradas ou se ocorrerem determinados tipos de oscilação. Se uma conta exigir uma atualização, o status da conta mostrará Atualização disponível na página Contas.

  Para atualizar uma única conta, navegue até a página de detalhes da conta e selecione Atualizar conta. As contas também podem ser atualizadas por meio de um processo manual, escolhendo Registrar novamente a OU ou com uma abordagem de script automatizada, descrita em uma seção posterior desta página.
- Uma atualização completa: uma atualização completa inclui uma atualização da sua zona de destino, seguida de uma atualização de todas as contas registradas na sua UO registrada. Atualizações completas são necessárias com uma nova versão do AWS Control Tower, como 2.9, 3.0 e assim por diante.

> **Note**
>
> Depois de concluir uma atualização do landing zone, você não pode desfazer a atualização ou fazer o downgrade para uma versão anterior.

# Atualize sua landing zone

A maneira mais fácil de atualizar sua zona de pouso da AWS Control Tower é por meio da página de configurações da zona de pouso, que você pode acessar escolhendo as configurações da zona de pouso na navegação à esquerda do painel da AWS Control Tower.

A página de configurações da zona de pouso mostra a versão atual da sua zona de pouso e lista todas as versões atualizadas que possam estar disponíveis. É possível escolher o botão Update (Atualizar) se precisar atualizar a versão.

> **Note**
>
> Como alternativa, é possível atualizar a zona de destino manualmente. A atualização leva aproximadamente a mesma quantidade de tempo, se você usar o botão Update (Atualizar) ou o processo manual. Para executar uma atualização manual somente da zona de destino, consulte as etapas 1 e 2 a seguir.

## Procedimento de atualização padrão

O procedimento a seguir mostra as etapas de uma atualização completa do AWS Control Tower a partir do console. Para atualizar uma conta individual, consulteAtualize a conta no console.

Para atualizar sua landing zone, com qualquer número de contas por OU

1. Abra um navegador da Web e navegue até o console do AWS Control Tower em https://console.aws.amazon.com/controltower/home/update.
2. Examine as informações no assistente e escolha Update (Atualizar). Isso atualiza o back-end da landing zone, bem como suas contas compartilhadas. Esse processo pode levar um pouco mais de meia hora.
3. Atualize suas contas de membros (esse procedimento deve ser seguido para uma OU que contenha mais de 1000 contas).

4. No painel de navegação esquerdo, escolha Organização.
5. Para atualizar cada conta, siga as etapas fornecidas emAtualize a conta no console.

> Opcionalmente, registre novamente a OU para atualizar contas
>
> Para AWS Control Tower registrada OUs com menos de 300 contas, você pode ir até a página da OU no painel e selecionar Registrar a OU novamente para atualizar as contas nessa OU.

## Selecione uma versão da landing zone

Se você estiver executando a versão 3.1 e superior da zona de pouso do AWS Control Tower, você pode optar por permanecer na versão atual ou fazer o upgrade para uma versão mais nova ao realizar uma operação de atualização ou redefinição nas configurações da sua zona de pouso. A operação de reinicialização é a melhor maneira de reparar o desvio, na maioria das situações.

Você pode escolher uma versão de landing zone no console AWS Control Tower ou por meio da AWS Control TowerAPIs.

> Note
>
> Se você optar por implantar uma versão do landing zone que ignore uma versão intermediária, por exemplo, se você mudar da 3.1 para a 3.3, a AWS Control Tower implantará automaticamente a versão intermediária como parte da operação de atualização. Em uma conversa, mudar para uma versão mais recente costuma ser chamado de upgrade, não apenas de atualização. Esses dois conceitos são distintos, pois você pode atualizar suas configurações de landing zone sem precisar fazer o upgrade para uma nova versão, por exemplo, alterando as regiões que você governa. No console, o botão Atualizar executa uma atualização local ou uma operação de upgrade, com base na sua versão atual do landing zone e na que você selecionou para implantar.

Escolha sua versão do landing zone — procedimento do console

1. No console do AWS Control Tower, navegue até a página de configurações da zona de pouso. Na tabela de zonas de pouso disponíveis, selecione a nova versão. Lembre-se de que você

pode selecionar as versões 3.1 ou posteriores. As versões anteriores à 3.1 não são compatíveis com esse recurso.

2. Ao selecionar uma versão da tabela, você pode ver as ações disponíveis. A atualização estará disponível se sua versão atual for anterior à versão selecionada. A redefinição está disponível se sua versão atual for 3.1 ou mais recente.
3. Depois de escolher a versão, selecione o botão Atualizar ou o botão Redefinir, na área superior direita da tela.
4. Você verá uma tela de confirmação mostrando a versão do landing zone que você selecionou para implantação. Para continuar, escolha Avançar no canto inferior direito. Sua operação de atualização pode levar alguns minutos ou mais.
5. Depois que a landing zone for atualizada, talvez seja necessário atualizar suas contas. A maneira mais fácil de fazer as atualizações da conta é por meio do processo de novo registro da OU para cada um dos seus cadastradosOUs.

## Atualizações da conta, versões da landing zone e linhas de base

AWSAs zonas de pouso da Control Tower são AWS recursos que correspondem a um conjunto de configurações básicas. Não há um one-to-one mapeamento das linhas de base e das versões do landing zone. Você pode ver uma tabela que mostraCompatibilidade das linhas de base da OU e das versões do landing zone.

Ao pular uma versão básica, você deve atualizar as contas após a atualização da landing zone. Por exemplo, ao atualizar do 3.1 para o 3.2, você não precisaria atualizar suas contas, porque essas versões do landing zone compartilham a mesma linha de base.

Por outro lado, se você atualizar do 3.1 para o 3.3, precisará atualizar as contas, porque a versão básica é 4.0, que abrange 3.2 a 3.3.

Para obter mais informações sobre a relação entre as versões do landing zone e as linhas de base, consulte. Compatibilidade das linhas de base da OU e das versões do landing zone

## Esquemas de zona de aterrissagem

Uma landing zone é um AWS recurso criado por meio de esquemas. Cada versão da zona de pouso do AWS Control Tower tem um esquema exclusivo.

Os esquemas das zonas de pouso do AWS Control Tower, versão 3.0 e mais recentes, são publicados nesta seção de referência, para ajudá-lo a escolher uma versão compatível.

> **Note**
>
> Um problema conhecido relacionado ao registro de acesso desnecessário está presente na versão 3.0 do landing zone. O problema foi resolvido na versão 3.1 do landing zone. Para obter mais informações sobre as mudanças, consulteAWSVersão 3.1 da zona de pouso da Control Tower.

## Esquema da zona de pouso 3.1

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
```

```
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
```

```
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizatinalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                }
            },
            "additionalProperties": false
```

```
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

## Esquema da zona de pouso 3.2

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
```

```
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
```

```
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizatinalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
```

```
                "maxLength": 120,
                "minLength": 1,
                "pattern": "^[\\s\\S]*$",
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "OrganizationStructure": {
        "type": "object",
        "required": [
            "security"
        ],
        "properties": {
            "sandbox": {
                "$ref": "#/definitions/OrganizatinalUnit"
            },
            "security": {
                "$ref": "#/definitions/OrganizatinalUnit"
            }
        },
        "additionalProperties": false
    },
    "S3BucketConfiguration": {
        "type": "object",
        "properties": {
            "retentionDays": {
                "type": "number",
                "minimum": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "SecurityRoles": {
        "type": "object",
        "required": [
            "accountId"
        ],
        "properties": {
            "accountId": {
                "type": "string",
                "maxLength": 12,
                "minLength": 12,
```

```
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

## Esquema da zona de pouso 3.3

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
```

```
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
```

```
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizatinalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizatinalUnit"
                }
            },
            "additionalProperties": false
```

```
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

# Resolva o desvio com a redefinição e o registro novamente

A deriva geralmente ocorre quando você e os membros da sua organização usam a landing zone.

A detecção de deriva é automática na AWS Control Tower. As varreduras automatizadas SCPs ajudam você a identificar recursos que precisam de alterações ou atualizações de configuração que devem ser feitas para resolver o desvio.

Para reparar a maioria dos tipos de deriva, escolha Redefinir na página de configurações da zona de pouso. Além disso, você pode resolver alguns tipos de desvio escolhendo registrar novamente

uma OU. Para obter mais informações sobre os tipos de desvio e como resolvê-los, consulte Tipos de oscilação de governança e. Detecte e resolva desvios na AWS Control Tower

Um caso especial de resolução de desvio ocorre para o desvio de função. Se uma função necessária não estiver disponível, o console mostrará uma página de aviso e algumas instruções sobre como restaurar a função. Sua landing zone não estará disponível até que a mudança de função seja resolvida. Essa redefinição do drift não é a mesma que uma redefinição completa da landing zone. Para obter mais informações, consulte Não exclua as funções necessárias na seção chamadaTipos de desvio a serem resolvidos imediatamente.

⚠ Quando você toma medidas para resolver o desvio em uma versão de landing zone, dois comportamentos são possíveis.

- Se você estiver usando a versão mais recente da zona de pouso, ao escolher Redefinir e depois escolher Confirmar, os recursos da zona de pouso derivada serão redefinidos para a configuração salva da AWS Control Tower. A versão landing zone permanece a mesma.
- Se você não estiver usando a versão mais recente, deverá escolher Atualizar. A zona de pouso foi atualizada para a versão mais recente da zona de pouso. O desvio é resolvido como parte desse processo.

## Provisione e atualize contas usando automação

Você pode provisionar ou atualizar contas individuais no AWS Control Tower por vários métodos:

- Você pode provisionar e personalizar contas com o AWSControl Tower Account Factory for Terraform (AFT). Para obter mais informações, consulte Visão geral do AWS Control Tower Account Factory for Terraform () AFT.
- Você pode atualizar contas com Customizations for AWS Control Tower (cFct). Para obter mais informações, consulte Visão geral das personalizações do AWS Control Tower (cFct) .
- Automação de scripts: se você preferir usar uma API abordagem, você pode atualizar as contas usando a APIestrutura do Service Catalog e o AWS CLI para atualizar as contas em um processo em lote. Você chamaria o `UpdateProvisionedProduct`APIde Service Catalog para cada conta. Você pode escrever um script para atualizar as contas, uma por uma, com issoAPI. Mais informações sobre essa abordagem, ao adicionar regiões para governança, estão disponíveis em uma postagem no blog, Enabling guardrails in new AWS Regions.

Você pode atualizar até cinco (5) contas por vez. Você deve esperar que pelo menos uma atualização da conta seja bem-sucedida antes de iniciar a próxima atualização da conta. Portanto, o processo pode demorar bastante se você tiver muitas contas, mas não é complicado. Para obter mais informações sobre essa abordagem, consulte Passo a passo: Automatize o provisionamento de contas no AWS Control Tower por meio das APIs do Service Catalog.

> **Demonstração em vídeo**
>
> O foi Passo a passo em vídeo projetado para o provisionamento automatizado de contas com um script, mas as etapas também se aplicam à atualização da conta. Use o `UpdateProvisionedProduct` API em vez do `ProvisionProduct`API.

Uma etapa adicional da automação por script é verificar o status de Succeed do evento de `UpdateLandingZone` ciclo de vida da AWS Control Tower. Use-o como um gatilho para começar a atualizar contas individuais, conforme descrito no vídeo. Um evento de ciclo de vida marca a conclusão de uma sequência de atividades, portanto, a ocorrência desse evento significa que a atualização da landing zone foi concluída. A atualização da zona de destino deve ser concluída antes que as atualizações da conta sejam iniciadas. Para obter mais informações sobre como trabalhar com eventos de ciclo de vida, consulte Eventos de ciclo de vida.

Consulte também:

- Use AWS CloudShell para trabalhar com AWS Control Tower.
- Automatize tarefas no AWS Control Tower .

# Automatize tarefas no AWS Control Tower

Muitos clientes preferem automatizar tarefas no AWS Control Tower, como provisionamento de contas, atribuição de controle e auditoria. Você pode configurar essas ações automatizadas com chamadas para:

- AWS Service Catalog APIs
- AWS Organizations APIs
- APIs da AWS Control Tower
- a AWS CLI

A Informações e links adicionais página contém links para muitas publicações de blog técnicas excelentes que podem ajudar você a automatizar tarefas no AWS Control Tower. As seções a seguir fornecem links para áreas neste Guia do usuário do AWS Control Tower que podem ajudá-lo a automatizar tarefas.

Automatizando tarefas de controle

Você pode automatizar tarefas relacionadas à aplicação e remoção de controles (também conhecidos como grades de proteção) por meio da API AWS Control Tower. Para obter detalhes, consulte a referência da API do AWS Control Tower.

Para obter mais informações sobre como realizar operações de controle com as APIs da AWS Control Tower, consulte a postagem do blog AWS Control Tower lança API, controles predefinidos para suas unidades organizacionais.

Automatizando as tarefas da landing zone

As APIs da zona de pouso do AWS Control Tower ajudam você a automatizar determinadas tarefas relacionadas à sua zona de pouso. Para obter detalhes, consulte a referência da API do AWS Control Tower.

Automatizando o registro de OU

As APIs básicas do AWS Control Tower ajudam você a automatizar determinadas tarefas, como registrar uma OU. Para obter detalhes, consulte a referência da API do AWS Control Tower.

Encerramento automático da conta

Você pode automatizar o encerramento das contas dos membros do AWS Control Tower com uma AWS Organizations API. Para ter mais informações, consulte Feche uma conta de membro do AWS Control Tower por meio de AWS Organizations.

Provisionamento e atualização automatizados de contas

O AWS Control Tower Account Factory Customization (AFC) ajuda você a criar contas a partir do console da AWS Control Tower, com AWS CloudFormation modelos personalizados que chamamos de blueprints. Esse processo é automatizado no sentido de que você pode criar novas contas e atualizá-las repetidamente, depois de configurar um único blueprint, sem manter pipelines.

O AWS Control Tower Account Factory for Terraform (AFT) segue um GitOps modelo para automatizar os processos de provisionamento e atualização de contas na AWS Control Tower. Para ter mais informações, consulte Provisione contas com o AWS Control Tower Account Factory for Terraform (AFT) .

As personalizações do AWS Control Tower (cFct) ajudam você a personalizar sua zona de pouso da AWS Control Tower e a se manter alinhado com as melhores práticas. AWS As personalizações são implementadas com AWS CloudFormation modelos e políticas de controle de serviços (SCPs). Para ter mais informações, consulte Visão geral das personalizações do AWS Control Tower (cFct) .

Para obter mais informações e um vídeo sobre o provisionamento automatizado de contas, consulte Passo a passo: Provisionamento automático de contas no AWS Control Tower e Provisionamento automático com funções do IAM.

Consulte também Atualizar contas por script.

Auditoria programática de contas

Para obter mais informações sobre a auditoria programática de contas, consulte Funções programáticas e relações de confiança para a conta de auditoria do AWS Control Tower.

Automatizando outras tarefas

Para obter informações sobre como aumentar determinadas cotas de serviços do AWS Control Tower com um método de solicitação automatizado, assista a este vídeo: Automatize o aumento do limite de serviço.

Para blogs técnicos que abordam casos de uso de automação e integração, consulte Automação e integração.

Dois exemplos de código aberto estão disponíveis GitHub para ajudá-lo com determinadas tarefas de automação relacionadas à segurança.

- O exemplo chamado aws-control-tower-org-setup-sample mostra como automatizar a configuração da conta de auditoria como administrador delegado para serviços relacionados à segurança.
- O exemplo chamado aws-control-tower-account- setup-using-step-functions mostra como automatizar as melhores práticas de segurança usando Step Functions, ao provisionar e configurar novas contas. Esse exemplo inclui a adição de diretores a AWS Service Catalog portfólios compartilhados organizacionalmente e a associação automática de grupos do IAM Identity Center de toda a organização AWS a novas contas. Também ilustra como excluir a VPC padrão em cada região.

A arquitetura AWS de referência de segurança inclui exemplos de código para automatizar tarefas relacionadas ao AWS Control Tower. Para obter mais informações, consulte as páginas de orientação AWS prescritiva e o repositório associado GitHub .

Para obter informações sobre como usar o AWS Control Tower com AWS CloudShell, um AWS serviço que facilita o trabalho na AWS CLI, AWS CloudShell consulte e na AWS CLI.

Como o AWS Control Tower é uma camada de orquestração AWS Organizations, muitos outros AWS serviços estão disponíveis por meio de APIs e da CLI. AWS Para obter mais informações, consulte AWS Serviços relacionados.

## Use AWS CloudShell para trabalhar com AWS Control Tower

AWS CloudShell é um AWS serviço que facilita o trabalho no AWS CLI — é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do. AWS Management Console Não há necessidade de baixar ou instalar ferramentas de linha de comando. Você pode executar AWS CLI comandos para AWS Control Tower e outros AWS serviços a partir do shell de sua preferência (Bash PowerShell ou Z shell).

Quando você inicia a AWS CloudShell partir do AWS Management Console, AWS as credenciais que você usou para entrar no console estão disponíveis em uma nova sessão de shell. Você pode pular a inserção de suas credenciais de configuração ao interagir com outros AWS serviços AWS Control Tower e usará a AWS CLI versão 2, que está pré-instalada no ambiente computacional do shell. Você está pré-autenticado com. AWS CloudShell

# Obtenha IAM permissões para AWS CloudShell

AWS Identity and Access Management fornece recursos de gerenciamento de acesso que permitem que os administradores concedam permissões aos IAM usuários e aos usuários do IAM Identity Center para acesso a. AWS CloudShell

A maneira mais rápida de um administrador conceder acesso aos usuários é por meio de uma política AWS gerenciada. Uma política gerenciada pela AWS é uma política independente que é criada e administrada pela AWS. A seguinte política AWS gerenciada para CloudShell pode ser anexada às IAM identidades:

- `AWSCloudShellFullAccess`: concede permissão para uso AWS CloudShell com acesso total a todos os recursos.

Se você quiser limitar o escopo das ações que um IAM usuário ou usuário do IAM Identity Center pode executar AWS CloudShell, você pode criar uma política personalizada que usa a política `AWSCloudShellFullAccess` gerenciada como modelo. Para obter mais informações sobre como limitar as ações que estão disponíveis para os usuários em CloudShell, consulte Gerenciando o AWS CloudShell acesso e o uso com IAM políticas no Guia do AWS CloudShell usuário.

> **Note**
>
> Sua IAM identidade também exige uma política que conceda permissão para fazer chamadas para AWS Control Tower. Para obter mais informações, consulte Permissões necessárias para usar o AWS Control Tower console.

## Lançamento AWS CloudShell

A partir do AWS Management Console, você pode iniciar CloudShell escolhendo as seguintes opções disponíveis na barra de navegação:

- Escolha o CloudShell ícone.
- Comece a digitar “cloudshell” na caixa de pesquisa e escolha a opção. CloudShell

Agora que você começou CloudShell, pode inserir todos AWS CLI os comandos com os quais precisa trabalhar AWS Control Tower. Por exemplo, você pode verificar seu AWS Config status.

# Interaja com AWS Control Tower por meio de AWS CloudShell

Depois AWS CloudShell de iniciar a partir do AWS Management Console, você pode começar imediatamente a interagir com a interface AWS Control Tower da linha de comando. AWS CLI os comandos funcionam da maneira padrão em CloudShell.

> **Note**
>
> Ao usar o AWS CLI in AWS CloudShell, você não precisa baixar ou instalar nenhum recurso adicional. Você já está autenticado no shell, então não precisa configurar as credenciais antes de fazer chamadas.

Use AWS CloudShell para ajudar na configuração AWS Control Tower

Antes de realizar esses procedimentos, a menos que seja indicado de outra forma, você deve estar conectado AWS Management Console na região de origem da sua zona de pouso e estar conectado como um usuário do IAM Identity Center ou IAM usuário com permissões administrativas para a conta de gerenciamento que contém sua zona de pouso.

1. Veja como você pode usar AWS Config CLI comandos AWS CloudShell para determinar o status do seu gravador de configuração e do canal de entrega antes de começar a configurar sua AWS Control Tower landing zone.

   Exemplo: verifique seu AWS Config status

   Comandos de exibição:

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - A resposta normal é algo como `"name": "default"`

2. Se você tem um AWS Config gravador ou canal de entrega existente que precisa excluir antes de configurar sua AWS Control Tower landing zone, aqui estão alguns comandos que você pode inserir:

   Exemplo: gerencie seus recursos pré-existentes AWS Config

Comandos de exclusão:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

> **Important**
>
> Não exclua os AWS Control Tower recursos do AWS Config. A perda desses recursos pode causar AWS Control Tower a entrada em um estado inconsistente.

Para obter mais informações, consulte a AWS Config documentação

- Gerenciando o gravador de configuração ()AWS CLI
- Gerenciando o canal de entrega

3. Este exemplo mostra AWS CLI os comandos a partir dos quais você inseriria AWS CloudShell para ativar ou desativar o acesso confiável AWS Organizations. Pois AWS Control Tower você não precisa habilitar ou desabilitar o acesso confiável para AWS Organizations, é apenas um exemplo. No entanto, talvez seja necessário ativar ou desativar o acesso confiável para outros AWS serviços se estiver automatizando ou personalizando ações no. AWS Control Tower

   Exemplo: habilitar ou desabilitar o acesso a serviços confiáveis

   - `aws organizations enable-aws-service-access`
   - `aws organizations disable-aws-service-access`

Exemplo: Crie um bucket do Amazon S3 com AWS CloudShell

No exemplo a seguir, você pode usar AWS CloudShell para criar um bucket do Amazon S3 e, em seguida, usar o PutObjectmétodo para adicionar um arquivo de código como um objeto nesse bucket.

1. Para criar um bucket em uma AWS região específica, digite o seguinte comando na linha de CloudShell comando:

```
aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
```

Se a chamada tiver êxito, a linha de comando exibirá uma resposta do serviço semelhante à seguinte saída:

```
{
    "Location": "/insert-unique-bucket-name-here"
}
```

> **Note**
>
> Se você não seguir as regras para nomear intervalos (usando somente letras minúsculas, por exemplo), o seguinte erro será exibido: Ocorreu um erro (InvalidBucketName) ao chamar a CreateBucket operação: O intervalo especificado não é válido.

2. Para fazer upload de um arquivo e adicioná-lo como um objeto ao bucket que acabou de ser criado, chame o PutObject método:

```
aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
 add_prog.py
```

Se o objeto for carregado com sucesso no bucket do Amazon S3, a linha de comando exibirá uma resposta do serviço semelhante à seguinte saída:

```
{
           "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

`ETag`É o hash do objeto que foi armazenado. Ele pode ser usado para verificar a integridade do objeto carregado no Amazon S3.

# Crie AWS Control Tower recursos com AWS CloudFormation

AWS Control Tower é integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja, como `AWS::ControlTower::EnabledControl` controles. AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus AWS Control Tower recursos de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

## AWS Control Tower e AWS CloudFormation modelos

Para provisionar e configurar recursos AWS Control Tower e serviços relacionados, você deve entender AWS CloudFormation os modelos. Os modelos são arquivos de texto formatados em JSON ouYAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ouYAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar AWS CloudFormation modelos. Para obter mais informações, consulte O que é o AWS CloudFormation Designer? no Guia do usuário do AWS CloudFormation .

AWS Control Tower suporta a criação `AWS::ControlTower::EnabledControl` (recursos de controle), `AWS::ControlTower::LandingZone` (zonas de pouso) e `AWS::ControlTower::EnabledBaseline` (linhas de base) em. AWS CloudFormation Para obter mais informações, incluindo exemplos JSON e YAML modelos desses tipos de recursos, consulte AWS Control Towero Guia AWS CloudFormation do usuário.

> **Note**
>
> O limite `EnableControl` e as `DisableControl` atualizações AWS Control Tower são de 100 operações simultâneas, com até 20 dessas operações pertencentes a controles proativos.

Para ver alguns AWS Control Tower exemplos do CLI e do console, consulte Habilitar controles com AWS CloudFormation.

# Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- AWS CloudFormation APIReferência
- AWS CloudFormation Guia do usuário da interface de linha de comando

# Personalize sua zona de pouso do AWS Control Tower

Certos aspectos da sua zona de pouso do AWS Control Tower são configuráveis no console, como seleção de regiões e controles opcionais. Outras alterações podem ser feitas fora do console, com automação.

Por exemplo, você pode criar personalizações mais abrangentes da sua landing zone com o recurso Customizations for AWS Control Tower, uma estrutura de personalização no GitOps estilo que funciona com modelos e eventos do ciclo de vida do AWS AWS CloudFormation Control Tower.

## Personalize a partir do console do AWS Control Tower

Para fazer essas personalizações na sua landing zone, siga as etapas fornecidas pelo console do AWS Control Tower.

Selecione nomes personalizados durante a configuração

- Você pode selecionar seus nomes de OU de nível superior durante a configuração. Você pode renomear suas OUs a qualquer momento usando o AWS Organizations console, mas fazer alterações em suas OUs AWS Organizations pode causar desvios reparáveis.
- Você pode selecionar os nomes das suas contas compartilhadas de Auditoria e Arquivo de Registros, mas não pode alterar os nomes após a configuração. (Essa é uma seleção única.)

> **Dica**
>
> Lembre-se de que renomear uma OU em AWS Organizations não atualiza o produto provisionado correspondente no Account Factory. Para atualizar o produto provisionado automaticamente (e evitar desvios), você deve realizar a operação de OU por meio do AWS Control Tower, incluindo criar, excluir ou registrar novamente uma OU.

Selecionar AWS regiões

- Você pode personalizar sua landing zone selecionando AWS regiões específicas para governança. Siga as etapas no console do AWS Control Tower.

- Você pode selecionar e desmarcar AWS regiões para governança ao atualizar sua landing zone.
- Você pode definir o controle de negação de região como Ativado ou Não ativado e controlar o acesso do usuário à maioria dos AWS serviços em regiões não governadas AWS .

Para obter informações sobre Regiões da AWS onde o cFct tem limitações de implantação, consulteLimitações de controle.

Personalize adicionando controles opcionais

- Os controles eletivos e altamente recomendados são opcionais, o que significa que você pode personalizar o nível de fiscalização da sua landing zone escolhendo quais ativar. Os controles opcionais não estão habilitados por padrão.
- Os controles opcionais de residência de dados permitem que você personalize as regiões nas quais você armazena e permita o acesso aos seus dados.
- Os controles opcionais que fazem parte do padrão integrado do Security Hub permitem que você escaneie seu ambiente do AWS Control Tower para verificar os riscos de segurança.
- Os controles proativos opcionais permitem que você verifique seus AWS CloudFormation recursos antes de serem provisionados, para garantir que os novos recursos estejam em conformidade com os objetivos de controle do seu ambiente.

Personalize suas AWS CloudTrail trilhas

- Ao atualizar sua landing zone para a versão 3.0 ou posterior, você pode optar por participar ou não das CloudTrail trilhas em nível organizacional gerenciadas pelo AWS Control Tower. Você pode alterar essa seleção sempre que atualizar sua landing zone. O AWS Control Tower cria uma trilha em nível organizacional em sua conta de gerenciamento, e essa trilha entra no status ativo ou inativo, com base na sua escolha. A Landing zone 3.0 não suporta CloudTrail trilhas em nível de conta; no entanto, se você precisar delas, poderá configurar e gerenciar suas próprias trilhas. Você pode incorrer em custos adicionais por trilhas duplicadas.

Crie contas de membros personalizadas no console

- Você pode criar contas de membros do AWS Control Tower que são personalizadas e você pode atualizar contas de membros existentes para adicionar personalizações, a partir do console do AWS Control Tower. Para ter mais informações, consulte Personalize contas com Account Factory Customization (AFC).

# Automatize personalizações fora do console do AWS Control Tower

Algumas personalizações não estão disponíveis por meio do console do AWS Control Tower, mas podem ser implementadas de outras formas. Por exemplo: .

- Você pode personalizar contas durante o provisionamento, em um fluxo de trabalho no GitOps estilo -S, com o Account Factory for Terraform (AFT).

  O AFT é implantado com um módulo Terraform, disponível no repositório AFT.

- Você pode personalizar sua zona de pouso da AWS Control Tower com personalizações para a AWS Control Tower (cFct), um pacote de funcionalidades criado com base em AWS CloudFormation modelos e políticas de controle de serviços (SCPs). Você pode implantar os modelos e políticas personalizados em contas individuais e unidades organizacionais (OUs) em sua organização.

  O código-fonte do cFct está disponível em um GitHub repositório.

## Benefícios das personalizações para o AWS Control Tower (cFct)

O pacote de funcionalidades que chamamos de Customizations for AWS Control Tower (cFct) ajuda você a criar personalizações mais abrangentes para sua landing zone do que você pode criar no console do AWS Control Tower. Ele oferece um processo GitOps automatizado no estilo. Você pode remodelar sua landing zone para atender às suas necessidades comerciais.

Esse processo de infrastructure-as-codepersonalização integra AWS CloudFormation modelos com políticas de controle de AWS serviços (SCPs) e eventos do ciclo de vida do AWS Control Tower, para que suas implantações de recursos permaneçam sincronizadas com sua landing zone. Por exemplo, quando você cria uma nova conta com o Account Factory, os recursos vinculados à conta e à OU podem ser implantados automaticamente.

> **Note**
>
> Ao contrário do Account Factory e do AFT, o cFct não se destina especificamente a criar novas contas, mas a personalizar contas e OUs em sua landing zone, implantando recursos que você especificar.

Benefícios

- Expanda um AWS ambiente personalizado e seguro — Você pode expandir seu ambiente de várias contas do AWS Control Tower mais rapidamente e incorporar as AWS melhores práticas em um fluxo de trabalho de personalização repetível.
- Instancie seus requisitos — Você pode personalizar sua zona de pouso do AWS Control Tower de acordo com seus requisitos de negócios, com AWS CloudFormation modelos e políticas de controle de serviços que expressam suas intenções políticas.
- Automatize ainda mais com os eventos de ciclo de vida do AWS Control Tower — os eventos de ciclo de vida permitem que você implante recursos com base na conclusão de uma série anterior de eventos. Você pode contar com um evento de ciclo de vida para ajudá-lo a implantar recursos em contas e OUs automaticamente.
- Estenda sua arquitetura de rede — Você pode implantar arquiteturas de rede personalizadas que melhoram e protegem sua conectividade, como um gateway de trânsito.

## Exemplos adicionais de CFCT

- Um exemplo de caso de uso de rede com Customizations for AWS Control Tower (cFCT) é apresentado na postagem do blog AWS Architecture, Deploy consistent DNS with Service Catalog and AWS Control Tower customizations.
- Um exemplo específico relacionado ao cFct e à Amazon GuardDuty está disponível GitHub no `aws-samples`repositório.
- Exemplos de código adicionais relacionados ao cFCT estão disponíveis como parte da Arquitetura de Referência de AWS Segurança, no `aws-samples`repositório. Muitos desses exemplos contêm `manifest.yaml` arquivos de amostra em um diretório chamado`customizations_for_aws_control_tower`.

Para obter mais informações sobre a arquitetura AWS de referência de segurança, consulte as páginas de orientação AWS prescritiva.

## Visão geral das personalizações do AWS Control Tower (cFct)

As personalizações do AWS Control Tower (CFCt) ajudam você a personalizar sua zona de pouso da AWS Control Tower e a se manter alinhado com as melhores práticas. AWS As personalizações são implementadas com AWS CloudFormation modelos e políticas de controle de serviços ()SCPs.

Esse recurso cFct é integrado aos eventos do ciclo de vida do AWS Control Tower, para que suas implantações de recursos permaneçam sincronizadas com sua landing zone. Por exemplo, quando uma nova conta é criada por meio da fábrica de contas, todos os recursos vinculados à conta são implantados automaticamente. Você pode implantar os modelos e políticas personalizados em contas individuais e unidades organizacionais (OUs) em sua organização.

O vídeo a seguir descreve as melhores práticas para implantar um pipeline cFCT escalável e personalizações comuns de cFCT.

A seção a seguir fornece considerações arquitetônicas e etapas de configuração para a implantação do Customizations for Control Tower (AWScFct). Ele inclui um link para o AWS CloudFormationmodelo que inicia, configura e executa os AWS serviços necessários, de acordo com as AWS melhores práticas de segurança e disponibilidade.

Este tópico é destinado a arquitetos e desenvolvedores de infraestrutura de TI com experiência prática em arquitetura na AWS nuvem.

Para obter informações sobre as atualizações e alterações mais recentes nas Customizations for AWS Control Tower (cFct), consulte o CHANGELOGarquivo.md no repositório. GitHub

## Visão geral da arquitetura

A implantação do cFCT cria o seguinte ambiente na AWS nuvem, com um bucket Amazon S3 como fonte de configuração.

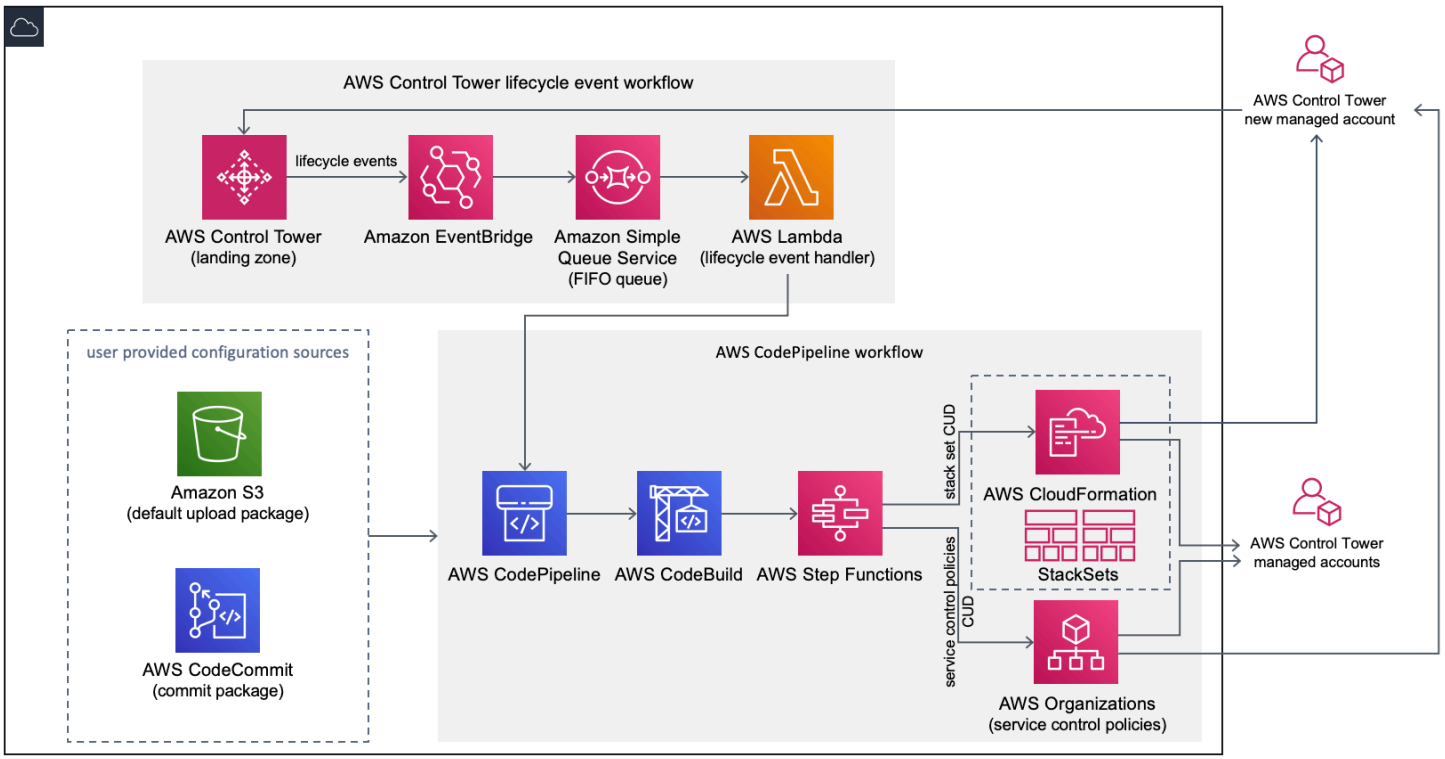


Figura 1: Personalizações da arquitetura AWS Control Tower

O cFct inclui um AWS CloudFormation modelo que você implanta na sua conta de gerenciamento da AWS Control Tower. O modelo inicia todos os componentes necessários para criar os fluxos de trabalho, para que você possa personalizar sua landing zone da AWS Control Tower.

> **Observação**
>
> O CFCt deve ser implantado na região de origem da AWS Control Tower e na conta de gerenciamento da AWS Control Tower, porque é aí que sua zona de pouso da AWS Control Tower está implantada. Para obter informações sobre como configurar uma landing zone da AWS Control Tower, consulteConceitos básicos.

Conforme você implanta o cFct, ele empacota e carrega os recursos personalizados na fonte do pipeline de código, por meio do Amazon Simple Storage Service (Amazon S3). O processo de upload invoca automaticamente a máquina de estado das políticas de controle de serviço (SCPs) e a máquina de AWS CloudFormation StackSetsestado para implantá-las SCPs no nível da OU ou para implantar instâncias de pilha no nível da OU ou da conta.

> **Observação**
>
> Por padrão, o cFct cria um bucket do Amazon S3 para armazenar a origem do pipeline. Se você tiver um AWS CodeCommit repositório existente, poderá alterar o local para um CodeCommitrepositório. Para obter mais informações, consulte Configurar o Amazon S3 como fonte de configuração.

O cFct implanta dois fluxos de trabalho:

- um AWS CodePipelinefluxo de trabalho
- e um fluxo de trabalho AWS de eventos de ciclo de vida da Control Tower.

O AWS CodePipeline fluxo de trabalho

O AWS CodePipeline fluxo de trabalho configura AWS CodePipeline, AWS CodeBuildprojeta e AWS Step Functionsorquestra o gerenciamento de AWS CloudFormation StackSets e SCPs em sua organização.

Quando você carrega o pacote de configuração, o cFct invoca o pipeline de código para executar três estágios.

- Build Stage — valida o conteúdo do pacote de configuração usando AWS CodeBuild.
- SCPEstágio — invoca a máquina de estado da política de controle de serviço, que chama o AWS Organizations API to create. SCPs
- AWS CloudFormation Etapa — invoca a máquina de estado do conjunto de pilhas para implantar os recursos especificados na lista de contas ouOUs, que você forneceu no arquivo de manifesto.

Em cada estágio, o pipeline de código invoca o conjunto de pilhas e as funções de SCP etapas, que implantam conjuntos de pilhas personalizados nas contas individuais de destino ou em uma unidade organizacional inteira. SCPs

> **Observação**
>
> Para obter informações detalhadas sobre a personalização do pacote de configuração, consulte. Guia de personalização do cFct

O fluxo de AWS trabalho do evento do ciclo de vida da Control Tower

Quando uma nova conta é criada no AWS Control Tower, um evento de ciclo de vida pode invocar o fluxo de trabalho. AWS CodePipeline Você pode personalizar o pacote de configuração por meio desse fluxo de trabalho, que consiste em uma regra de EventBridge evento da Amazon, uma fila de primeiro a entrar, primeiro a sair (SQS) do Amazon Simple Queue Service (AmazonFIFO) e uma função. AWS Lambda

Quando a regra de EventBridge eventos da Amazon detecta um evento de ciclo de vida correspondente, ela passa o evento para a SQS FIFO fila da Amazon, invoca a AWS Lambda função e invoca o pipeline de código para realizar a implantação posterior de conjuntos de pilhas e. SCPs

## Custo

O custo da execução do cFct depende do número de AWS CodePipeline execuções, da duração das AWS CodeBuild execuções, do número e da duração das AWS Lambda funções e do número de EventBridge eventos da Amazon publicados. Por exemplo, se você executar 100 compilações em um mês usando build.general1.small em que cada compilação é executada por cinco minutos, o custo aproximado da execução do cFct é de 3,00 USD por mês. Para obter detalhes completos, consulte a página de preços de cada AWS serviço que você está executando.

O bucket do Amazon Simple Storage Service (Amazon S3) AWS CodeCommit e os recursos do repositório baseados em Git são retidos após a exclusão do modelo, para proteger suas informações de configuração. Dependendo da opção selecionada, você será cobrado com base na quantidade de dados armazenados no bucket do Amazon S3 e no número de solicitações do Git (não aplicável ao recurso do Amazon S3). Consulte o Amazon S3 e os AWS CodeCommitpreços para obter detalhes.

# Serviços de componentes

Os AWS serviços a seguir são componentes do Customizations for AWS Control Tower (cFct).

## AWS CodeCommit

Se você tiver um AWS CodeCommit repositório existente, poderá configurá-lo como uma fonte para seu pipeline, como alternativa ao Amazon S3.

Com base na sua entrada no AWS CloudFormation modelo, o cFct pode criar um AWS CodeCommitrepositório com o mesmo exemplo de configuração explicado na seção Amazon Simple Storage Service.

Para clonar o AWS CodeCommit repositório cFCT em seu computador local, você deve criar credenciais que forneçam acesso temporário ao repositório, conforme explicado no Guia do usuário.AWS CodeCommit Para obter informações sobre compatibilidade de versões, consulte Configurando para AWS CodeCommit.

> **Note**
>
> Se você ainda não usa CodeCommit, sua única opção é configurar o bucket do Amazon S3 como o local de armazenamento do seu pacote de configuração. CodeCommit não está disponível se você estiver implantando o cFCT pela primeira vez.

## AWS CodePipeline

AWS CodePipeline valida, testa e implementa alterações com base nas atualizações do pacote de configuração, que você fará no bucket padrão do Amazon S3 ou no repositório. AWS CodeCommit Para obter mais informações sobre o controle da fonte de configuração, consulte Usando o Amazon S3 como fonte de configuração. O pipeline inclui estágios para validar e gerenciar os arquivos e modelos de configuração, contas principais, políticas AWS Organizations de controle de serviços e. AWS CloudFormation StackSets Para obter mais informações sobre os estágios do pipeline, consulte Guia de personalização do cFct

## AWS Key Management Service

O cFct cria uma chave de `CustomControlTowerKMSKey` criptografia AWS Key Management Service(AWS KMS). Essa chave é usada para criptografar objetos no bucket de configuração do Amazon S3, na fila da SQS Amazon e em parâmetros confidenciais no Systems AWS Manager Parameter Store. Por padrão, somente as funções provisionadas pelo cFct têm permissão para realizar operações de criptografia ou descriptografia com essa chave. Para acessar o arquivo de configuração, a FIFO fila ou `SecureString` os valores do Parameter Store, os administradores devem ser adicionados à `CustomControlTowerKMSKey` política. A rotação automática de chaves está ativada por padrão.

## AWS Lambda

O cFct usa AWS Lambda funções para invocar os componentes de instalação durante a instalação e implantação iniciais de AWS CloudFormation StackSets ou AWS Organizations SCPs durante um evento de ciclo de vida da AWS Control Tower.

## Amazon Simple Notification Service

O CfCT pode publicar notificações, como aprovação de pipeline para tópicos do Amazon Simple Notification Service (AmazonSNS) durante o fluxo de trabalho. A Amazon SNS é lançada somente quando você escolhe receber notificações de aprovação do funil.

## Amazon Simple Storage Service

Quando você implanta o cFCT, o cFct cria um bucket do Amazon Simple Storage Service (Amazon S3) com um nome exclusivo:

Exemplo: nome do bucket do Amazon S3

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

O bucket contém um exemplo de arquivo de configuração chamado `_custom-control-tower-configuration.zip`

Observe o sublinhado inicial no nome do arquivo.

Esse arquivo zip fornece um exemplo de manifesto e os modelos de amostra relacionados que descrevem a estrutura de pastas necessária. Esses exemplos ajudam você a desenvolver um pacote de configuração para personalizar sua zona de pouso do AWS Control Tower. O exemplo de manifesto identifica as configurações necessárias para conjuntos de pilhas e políticas de controle de serviço (SCPs) que você precisará ao implementar suas personalizações.

Você pode usar esse pacote de configuração de amostra como modelo para desenvolver e carregar seu pacote personalizado, que aciona o pipeline de configuração do cFct automaticamente.

Para obter informações sobre como personalizar o arquivo de configuração, consulteGuia de personalização do cFct.

## Amazon Simple Queue Service

O cFct usa uma fila do Amazon Simple Queue Service SQS (Amazon) para capturar FIFO eventos de ciclo de vida da Amazon. EventBridge Ele aciona uma AWS Lambda função, que invoca AWS CodePipeline para implantar ou. AWS CloudFormation StackSets SCPs Para obter mais informações sobreSCPs, consulte AWS Organizations.

### AWS Step Functions

O cFct cria Step Functions para orquestrar implantações de personalização. Essas Step Functions traduzem arquivos de configuração para implantar as personalizações conforme necessário em todos os ambientes.

### AWS Armazenamento de parâmetros do Systems Manager

AWSO Systems Manager Parameter Store armazena os parâmetros de configuração do cFct. Esses parâmetros permitem que você integre modelos de configuração relacionados. Por exemplo, você pode configurar cada conta para registrar AWS CloudTrail dados em um bucket centralizado do Amazon S3. Além disso, o Systems Manager Parameter Store fornece um local centralizado onde os administradores podem visualizar as entradas e os parâmetros do cFCT.

## Considerações de implantação

Certifique-se de iniciar o Customizations for AWS Control Tower (cFct) na mesma conta e região em que sua landing zone da AWS Control Tower está implantada; ou seja, você deve implantá-la na conta de gerenciamento da Control Tower AWS na sua região de origem da Control TowerAWS. Por padrão, o cFct cria e executa o pacote de configuração do landing zone configurando um pipeline de configuração nessa conta e região.

### Preparar-se para implantação

Você tem algumas opções ao preparar seu AWS CloudFormation modelo para a implantação inicial. Você pode escolher a fonte de configuração e permitir a aprovação manual das implantações do pipeline. As próximas duas seções explicam mais sobre essas opções.

#### Escolha sua fonte de configuração

Por padrão, o modelo cria um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar o pacote de configuração de amostra como `.zip` um arquivo chamado. `_custom-control-tower-configuration.zip` O bucket do Amazon S3 tem controle de versão e você pode atualizar o pacote de configuração conforme necessário. Para obter informações sobre a atualização do pacote de configuração, consulte Usando o Amazon S3 como fonte de configuração.

> **Lembre-se de remover o sublinhado**
>
> O nome do arquivo do pacote de configuração de amostra começa com um sublinhado (_) para que não AWS CodePipeline seja iniciado automaticamente. Quando terminar de personalizar o pacote de configuração, certifique-se de fazer o upload do `custom-control-tower-configuration.zip` sem o sublinhado (_) para iniciar a implantação em. AWS CodePipeline

Se você tiver um repositório AWS CodeCommit Git existente, poderá alterar o local de armazenamento do pacote de configuração do bucket do Amazon S3 para um repositório Git. AWS CodeCommit Para fazer isso, selecione a `CodeCommit` opção no AWS CloudFormation parâmetro.

> **Fechar ou não fechar?**
>
> Ao usar o bucket padrão do S3, certifique-se de que o pacote de configuração esteja disponível como um `.zip` arquivo. Se você estiver usando o AWS CodeCommit repositório, certifique-se de colocar o pacote de configuração no repositório sem compactar os arquivos. Para obter informações sobre como criar e armazenar o pacote de configuração em AWS CodeCommit, consulteGuia de personalização do cFct.

Você pode usar o pacote de configuração de amostra para criar sua própria fonte de configuração personalizada. Quando você estiver pronto para implantar suas configurações personalizadas, faça o upload manual do pacote de configuração para o bucket do Amazon S3 ou para AWS CodeCommit o repositório. O pipeline começa automaticamente quando você carrega o arquivo de configuração.

## Escolha seus parâmetros de aprovação de configuração de tubulação

O AWS CloudFormation modelo oferece a opção de aprovar manualmente a implantação das alterações de configuração. Por padrão, a aprovação manual não está habilitada. Para obter mais informações, consulte a Etapa 1. Lance a pilha.

Quando a aprovação manual é ativada, o pipeline de configuração valida as personalizações feitas no manifesto e nos modelos de arquivos do AWS Control Tower e, em seguida, pausa o processo até que a aprovação manual seja concedida. Após a aprovação, a implantação prossegue com a execução das etapas restantes do pipeline, conforme necessário, para implementar a funcionalidade Customizations for AWS Control Tower (cFCT).

Você pode usar o parâmetro de aprovação manual para impedir que as personalizações da configuração do AWS Control Tower sejam executadas, rejeitando a primeira tentativa de executar o pipeline. Esse parâmetro também permite validar manualmente as personalizações das alterações de configuração do AWS Control Tower, como controle final antes da implementação.

### Para atualizar as personalizações do Control Tower AWS

Se você já implantou o cFCT, você deve atualizar a AWS CloudFormation pilha para obter a versão mais recente da estrutura do cFCT. Para obter detalhes, consulte Atualizar a pilha.

## Modelo e código-fonte

As personalizações do AWS Control Tower (cFCT) são implantadas em sua conta de gerenciamento depois que você lança seu modelo. AWS CloudFormation Você pode baixar o modelo GitHub e, em seguida, iniciá-lo a partir de AWS CloudFormation.

O customizations-for-aws-control-tower.template implanta o seguinte:

- Um AWS CodeBuild projeto
- Um AWS CodePipeline projeto
- Uma EventBridge regra da Amazon
- AWS Lambda funções
- Uma fila do Amazon Simple Queue Service
- Um bucket do Amazon Simple Storage Service com um pacote de configuração de amostra
- AWS Step Functions

> **Note**
>
> Você pode personalizar o modelo com base em seus requisitos específicos.

### Repositório de código-fonte

Você pode visitar nosso GitHubrepositório para baixar os modelos e scripts do cFct e compartilhar as personalizações da sua landing zone com outras pessoas.

# Implantação automatizada

Antes de iniciar a implantação automatizada, analise as considerações. Siga as step-by-step instruções nesta seção para configurar e implantar a solução em sua conta de gerenciamento da AWS Control Tower.

Tempo de implantação: aproximadamente 15 minutos

## Pré-requisitos

O cFct deve ser implantado em sua conta de gerenciamento da AWS Control Tower e em sua região de origem da AWS Control Tower. Se você não tiver uma landing zone configurada, consulteConceitos básicos.

## Etapas da implantação

O procedimento para implantar o cFCT consiste em duas etapas principais. Para obter instruções detalhadas, siga os links para cada etapa.

Etapa 1. Iniciar a pilha do

- Inicie o AWS CloudFormation modelo em sua conta de gerenciamento.
- Revise os parâmetros do modelo e ajuste, se necessário.

Etapa 2. Crie um pacote personalizado

- Crie um pacote de configuração personalizado.

> **Important**
>
> Para baixar o AWS CloudFormation modelo correto e iniciar o cFct, siga o GitHub link fornecido nesta seção. Não siga links antigos para nenhum bucket do S3 especificado anteriormente.

## Etapa 1. Iniciar a pilha do

O AWS CloudFormation modelo nesta seção implanta Customizations for AWS Control Tower (cFct) em sua conta.

> **Observação**
>
> Você é responsável pelo custo dos AWS serviços usados enquanto executa o cFct. Para obter mais detalhes, consulte Custo.

1. Para iniciar o Customizations for AWS Control Tower, baixe o modelo GitHub e, em seguida, inicie-o em. AWS CloudFormation
2. Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia). Para iniciar o cFct em uma AWS região diferente, use o seletor de região na barra de navegação do console.

   > **Note**
   >
   > O CFct deve ser lançado na mesma região e conta em que você implantou sua landing zone da AWS Control Tower, que é sua região natal.

3. Na página Criar pilha, verifique se o modelo correto URL aparece na caixa de URLtexto e escolha Avançar.
4. Na página Especificar detalhes da pilha, atribua um nome à sua pilha cFct.
5. Em Parâmetros, revise os parâmetros a seguir e modifique-os no modelo, se necessário.

| Configuração do pipeline | | |
|---|---|---|
| Parâmetro | Padrão | Descrição |
| Estágio de aprovação do pipeline | No | Escolha se deseja alterar a configuração do pipeline do estágio de aprovação automatizada padrão para um estágio de aprovação manual. Para obter mais informações, consulte the section called “Guia de personalização do cFct”. |
| Endereço de e-mail de aprovação do pipeline | <Optional Input> | O endereço de e-mail para notificações de aprovação |

| Configuração do pipeline | | |
|---|---|---|
| Parâmetro | Padrão | Descrição |
| | | . Para usar esse parâmetro , você deve definir o parâmetro Pipeline Approval Stage como`Yes`. |
| AWS CodePipelineFonte | `Amazon S3` | A fonte AWS CodePipeline para ajudá-lo a selecionar onde armazenar e configurar as personalizações do cFct. |
| AWS CodeCommit Configuração | | |
| Parâmetro | Padrão | Descrição |
| CodeCommitRepositório existente? | `No` | Escolha se deseja usar um repositório CodeCommi t Git existente. Se você escolher`Yes`, defina o parâmetro CodePipel ine Source como`AWS CodeCommit` . |
| CodeCommit Nome do repositório | `custom-control-tow er-configuration` | Se você fornecer o nome de um repositório Git existente , deverá definir o Repositór io existente? CodeCommi t parâmetro `Yes` e insira o nome exato desse repositór io. |

| AWS CodeCommit Configuração | | |
|---|---|---|
| Parâmetro | Padrão | Descrição |
| CodeCommit Nome da filial | `main` | A ramificação do Git em que o pacote de personalização é armazenado. Para usar esse parâmetro, você deve definir o parâmetro CodePipeline Source como`AWS CodeCommit` . |
| **AWS CloudFormation StackSets Configuração** | | |
| Parâmetro | Padrão | Descrição |
| Tipo de concorrência de região | `PARALLEL` | Selecione o tipo de simultaneidade das StackSets operações de implantação nas regiões. Essa configuração é aplicável para criar, atualizar e excluir fluxos de trabalho. Outro valor permitido é`SEQUENTIAL` . |
| Porcentagem máxima simultânea | `100` | A porcentagem máxima de contas em que essa operação pode ser executada ao mesmo tempo. O valor máximo permitido é 100. Para obter mais informações, consulte as opções de operação do Stack Set. |

| AWS CloudFormation StackSets Configuração | | |
|---|---|---|
| Parâmetro | Padrão | Descrição |
| Porcentagem de tolerância a falhas | `10` | A porcentagem de contas, por região, nas quais essa operação de pilha pode falhar antes de AWS CloudFormation interromper a operação nessa região. O valor mínimo permitido é 0 e o valor máximo permitido é 100. Para obter mais informações, consulte as opções de operação do Stack Set. |

6. Escolha Próximo.
7. Na página Configurar opções de pilha, selecione Avançar.
8. Na página Revisar, verifique e confirme as configurações. Certifique-se de marcar a caixa confirmando que o modelo criará recursos AWS Identity and Access Management (IAM).
9. Selecione Create stack (Criar pilha) para implantar a pilha.

   Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve ver um status de CREATE_ COMPLETE em aproximadamente 15 minutos.

## Etapa 2. Crie um pacote personalizado

Com a pilha lançada, você pode adicionar personalizações à sua zona de pouso e às políticas de AWS controle de serviço (SCPs) da Control Tower personalizando o pacote de configuração incluído. Para obter instruções detalhadas sobre como criar um pacote personalizado, consulte Guia de personalização do cFct o.

> **Observação**
>
> O pipeline não é executado sem o upload do pacote de configuração personalizado.

# Atualize a pilha

Se você implantou anteriormente o Customizations for AWS Control Tower (cFCT), siga o procedimento para atualizar a AWS CloudFormation pilha para a versão mais recente da estrutura cFCT.

> **Important**
>
> Antes de concluir o procedimento a seguir, você deve fazer o upload do modelo mais recente em um GitHub bucket do Amazon Simple Storage Service (Amazon S3). Para obter instruções sobre como começar a usar o Amazon S3, consulte Introdução ao Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

1. Faça login no console do AWS CloudFormation.
2. Selecione sua CloudFormation pilha existente de Customizations for AWS Control Tower (cFct) e selecione Atualizar.
3. Em Pré-requisito — Preparar modelo, selecione Substituir modelo atual.
4. Em Especificar modelo, faça o seguinte:
   a. Em Fonte do modelo, selecione Substituir modelo atual.
   b. Para o Amazon S3 URL, insira o modelo do qual você fez o upload anteriormente URL para o Amazon S3 e, em seguida, escolha Avançar. GitGub
   c. Verifique se o modelo URL está correto. Em seguida, escolha Avançar e Avançar novamente.
5. Em Parâmetros, revise os parâmetros do modelo e modifique-os conforme necessário. Consulte a Etapa 1. Inicie a pilha para obter detalhes sobre os parâmetros.
6. Escolha Próximo.
7. Na página Configurar opções de pilha, selecione Avançar.
8. Na página Revisar, verifique e confirme as configurações. Certifique-se de marcar a caixa confirmando que o modelo pode criar recursos AWS Identity and Access Management (IAM).
9. Escolha Exibir conjunto de alterações e verifique as alterações.
10. Selecione Criar pilha para implantar a pilha.

    Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você deve ver um status de UPDATE_ COMPLETE em aproximadamente 15 minutos.

# Excluir um conjunto de pilhas

Você pode excluir um conjunto de pilhas se tiver ativado a exclusão do conjunto de pilhas no arquivo de manifesto. Por padrão, o parâmetro `enable_stack_set_deletion` é definido como `false`. Nessa configuração, nenhuma ação é tomada para excluir o conjunto de pilhas associado quando um recurso é removido do arquivo de manifesto cFct.

Se você alterar o valor de `enable_stack_set_deletion` to `true` no arquivo de manifesto, o cFct excluirá o conjunto de pilhas e todos os seus recursos ao remover um recurso associado do arquivo de manifesto.

Esse recurso é suportado na v2 do arquivo de manifesto.

> **Important**
>
> Quando você define inicialmente o valor de `enable_stack_set_deletion` para`true`, na próxima vez que invocar o cFct, ALLos recursos que começam com o prefixo`CustomControlTower-`, que têm a tag `Key:AWS_Solutions, Value: CustomControlTowerStackSet` de chave associada e que não são declarados no arquivo de manifesto, são preparados para exclusão.

Aqui está um exemplo de como definir esse parâmetro em um `manifest.yaml` arquivo:

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2
```

```
- name: demo_resource_2
  resource_file: s3://demo_bucket/resource.template
  deployment_targets:
    accounts:
      - 012345678912
  deploy_method: stack_set
  ...
  regions:
  - us-east-1
  - eu-north-1
```

## Configure o Amazon S3 como fonte de configuração

Quando você configura personalizações para o AWS Control Tower, ele armazena um arquivo de configuração inicial, chamado `_custom-control-tower-configuration.zip` arquivo, em um bucket do Amazon Simple Storage Service (Amazon S3), chamado. `custom-control-tower-configuration-`*`account-ID`*`-`*`region`*

> **Observação**
>
> Se você optar por baixar e modificar esse arquivo, lembre-se de compactar as alterações, salvar como um novo arquivo chamado `ecustom-control-tower-configuration.zip`, em seguida, enviá-lo de volta para o mesmo bucket do Amazon S3.
> O bucket do Amazon S3 é a fonte padrão do pipeline. Quando as configurações padrão estiverem definidas, o upload de um arquivo zip de configuração sem o prefixo de sublinhado no nome do arquivo para o bucket do S3 iniciará o pipeline automaticamente.

O arquivo zip é protegido pela criptografia do lado do servidor (SSE) com AWS Key Management Service (AWS KMS) e pela negação do uso da chave KMS. Para acessar o arquivo zip, você deve atualizar a Política de Chaves do KMS para especificar as funções que devem receber acesso. A função pode ser de administrador, usuário ou ambas. Siga este procedimento:

1. Navegue até o console doAWS Key Management Service.
2. Em Chaves gerenciadas pelo cliente, selecione CustomControlTowerKMSKey.
3. Selecione a guia Política de chaves. Em seguida, selecione Editar.

4. Na página Editar política de chaves, encontre a seção Permitir o uso da chave no código e adicione uma das seguintes permissões:
   - Para adicionar uma função administrativa:

     `arn:aws:iam::<account-ID>:role/<administrator-role>`
   - Para adicionar um usuário:

     `arn:aws:iam::<account-ID>:user/<username>`
5. Escolha Save Changes (Salvar alterações).
6. Navegue até o console do Amazon S3, encontre o bucket do S3 contendo o arquivo zip de configuração e selecione download.
7. Faça as alterações de configuração necessárias no arquivo de manifesto e nos arquivos de modelo. Para obter informações sobre como personalizar os arquivos de manifesto e modelo, consultethe section called “Guia de personalização do cFct”.
8. Faça o upload de suas alterações:
   a. Compacte os arquivos de configuração modificados e nomeie o arquivo:`custom-control-tower-configuration.zip`.
   b. Faça o upload do arquivo para o Amazon S3 usando SSE com a chave AWS KMS mestra:. `CustomControlTowerKMSKey`

# Coleção de métricas operacionais

As personalizações do AWS Control Tower (cFct) incluem uma opção para enviar métricas operacionais anônimas para. AWS AWS usa esses dados para entender como os clientes estão usando o cFct, bem como outros serviços e produtos relacionados. Quando a coleta de dados é ativada, as seguintes informações são enviadas para AWS:

- ID da solução: o identificador da AWS solução
- ID exclusivo (UUID): identificador exclusivo gerado aleatoriamente para cada implantação
- Carimbo de data e hora: data e hora da coleta de dados
- Contagem de execuções da máquina de estado: conta incrementalmente o número de vezes que essa máquina de estado é executada
- Versão do manifesto: a versão do manifesto usada na configuração

> **Note**
>
> AWS possui os dados que coleta. A coleta de dados está sujeita à AWS Política de Privacidade.

Para optar por não enviar métricas operacionais anônimas para AWS, conclua uma das seguintes tarefas:

- Atualize a seção AWS CloudFormation de mapeamento do modelo da seguinte forma:

  de

  ```
  AnonymousData:
       SendAnonymousData:
          Data: Yes
  ```

  para

  ```
  AnonymousData:
       SendAnonymousData:
          Data: No
  ```

- Depois que o cFct for implantado, localize a chave do parâmetro **`/org/primary/metrics_flag`** SSM no console do Parameter Store e atualize o valor para. **`No`**

# Guia de personalização do cFct

O guia Customizations for AWS Control Tower (cFCT) é para administradores, DevOps profissionais, fornecedores independentes de software, arquitetos de infraestrutura de TI e integradores de sistemas que desejam personalizar e ampliar seus ambientes de Control Tower AWS para suas empresas e clientes. Ele fornece informações sobre como personalizar e ampliar o ambiente AWS Control Tower com o pacote de personalização cFct.

> **Note**
>
> Para implantar e configurar (cFct), você deve implantar e processar um pacote de configuração por meio AWS CodePipeline de. As seções a seguir descrevem o processo em detalhes.

## Visão geral do pipeline de código

O pacote de configuração requer o Amazon Simple Storage Service (Amazon S3) e. AWS CodePipeline O pacote de configuração contém os seguintes itens:

- Um arquivo de manifesto
- Um conjunto de modelos que o acompanha
- Outros JSON arquivos para descrever e implementar suas personalizações do ambiente AWS Control Tower

Por padrão, o pacote de `_custom-control-tower-configuration.zip` configuração é carregado em um bucket do Amazon S3 com a seguinte convenção de nomenclatura:

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> Por padrão, o cFct cria um bucket do Amazon S3 para armazenar a origem do pipeline. A maioria dos clientes permanece com esse padrão. Se você tiver um AWS CodeCommit repositório existente, poderá alterar o local de origem do seu AWS CodeCommit repositório. Para obter mais informações, consulte Editar um pipeline CodePipeline no Guia AWS CodePipeline do usuário.

O arquivo de manifesto é um arquivo de texto que descreve os AWS recursos que você pode implantar para personalizar sua landing zone. CodePipeline executa as seguintes tarefas:

- extrai o arquivo de manifesto, o conjunto de modelos que o acompanha e outros arquivos JSON
- realiza validações de manifesto e modelo
- invoca seções no arquivo de manifesto para executar estágios específicos do pipeline.

Quando você atualiza o pacote de configuração personalizando o arquivo de manifesto e removendo o sublinhado (_) do nome do arquivo do pacote de configuração, ele é iniciado automaticamente. AWS CodePipeline

> **Lembre-se do sublinhado**
>
> O nome do arquivo do pacote de configuração de amostra começa com um sublinhado (_) para que não AWS CodePipeline seja acionado automaticamente. Quando você tiver concluído a personalização do pacote de configuração, faça o upload do arquivo `custom-control-tower-configuration.zip` sem o sublinhado (_) para acionar a implantação em. AWS CodePipeline

## AWS CodePipeline estágios

O pipeline do cFct requer vários AWS CodePipeline estágios para implementar e atualizar seu ambiente AWS Control Tower.

1. Estágio de origem

   O estágio de origem é o estágio inicial. Seu pacote de configuração personalizado inicia esse estágio do pipeline. A origem do AWS CodePipeline pode ser um bucket do Amazon S3 ou um AWS CodeCommit repositório, no qual o pacote de configuração pode ser hospedado.

2. Estágio de construção

   O estágio de construção exige AWS CodeBuild a validação do conteúdo do pacote de configuração. Essas verificações incluem testar a sintaxe e o esquema do `manifest.yaml` arquivo, junto com todos os AWS CloudFormation modelos incluídos no pacote ou hospedados remotamente, usando e. AWS CloudFormation `validate-template` `cfn_nag` Se o arquivo de manifesto e os AWS CloudFormation modelos passarem nos testes, o pipeline continuará para a próxima etapa. Se os testes falharem, você poderá revisar os CodeBuild registros para identificar o problema e editar o arquivo de origem da configuração conforme necessário.

3. Estágio de aprovação manual (opcional)

   O estágio de aprovação manual é opcional. Se você habilitar esse estágio, ele fornecerá controle adicional sobre o pipeline de configuração. Ele pausa o pipeline durante a implantação, até que uma aprovação seja dada. Você pode optar pela aprovação manual editando o parâmetro Pipeline Approval Stage como Sim ao iniciar a pilha.

4. Estágio da política de controle de serviços

   O estágio da política de controle de serviço invoca a máquina de estado da política de controle de serviço para chamar AWS Organizations APIs a criação de políticas de controle de serviço ()SCPs.

5. AWS CloudFormation estágio de recursos

   O estágio de AWS CloudFormation recursos invoca a máquina de estado do conjunto de pilhas para implantar os recursos especificados na lista de contas ou unidades organizacionais (OUs), que você forneceu no arquivo de manifesto. A máquina de estado cria os AWS CloudFormation recursos na ordem em que são especificados no arquivo de manifesto. Para especificar uma dependência de recursos, organize a ordem na qual os recursos são especificados no arquivo de manifesto. A ordem dos recursos no arquivo de manifesto é a única forma de especificar uma dependência.

## Definir uma configuração personalizada

Você definirá sua configuração personalizada da AWS Control Tower com o arquivo de manifesto, o conjunto de modelos que o acompanha e outros JSON arquivos. Você empacotará esses arquivos em uma estrutura de pastas e os colocará no bucket do Amazon S3 como um `.zip` arquivo, conforme mostrado no exemplo de código a seguir.

Estrutura de pastas de configuração personalizada

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

O exemplo anterior mostra a estrutura de uma pasta de configuração personalizada. A estrutura de pastas permanece a mesma, independentemente de você escolher o Amazon S3 ou um AWS CodeCommit repositório como local de armazenamento de origem. Se você escolher o Amazon S3 como armazenamento de origem, compacte todas as pastas e arquivos em um `custom-control-tower-configuration.zip` arquivo e carregue somente o `.zip` arquivo no bucket designado do Amazon S3.

> **Note**
>
> Se você estiver usando AWS CodeCommit, coloque os arquivos no repositório sem compactá-los.

## O arquivo de manifesto

O `manifest.yaml` arquivo é um arquivo de texto que descreve seus AWS recursos. O exemplo a seguir mostra a estrutura do arquivo de manifesto.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

Conforme mostrado no exemplo de código anterior, as duas primeiras linhas do arquivo de manifesto especificam os valores da região e as palavras-chave da versão. Aqui estão as definições dessas palavras-chave.

region — Uma sequência de texto para a região padrão da AWS Control Tower. Esse valor deve ser um nome de AWS região válido (como `us-east-1`eu-west-1, ou`ap-southeast-1`). A região inicial da AWS Control Tower é o padrão quando você cria recursos personalizados da AWS Control Tower (como AWS CloudFormation StackSets), a menos que uma região mais específica do recurso seja especificada.

```
region:your-home-region
```

versão — O número da versão do esquema do manifesto. A versão mais recente suportada é 2021-03-15.

```
version: 2021-03-15
```

> **Note**
>
> É altamente recomendável que você use a versão mais recente. Para atualizar as propriedades do manifesto na versão mais recente, consulteAtualizações da versão do manifesto.

A próxima palavra-chave mostrada no exemplo anterior é a palavra-chave resources. A seção de recursos do arquivo de manifesto é altamente estruturada. Ele contém uma lista detalhada de AWS recursos, que serão implantados automaticamente pelo pipeline cFct. Essas descrições dos recursos e seus parâmetros disponíveis são fornecidas na próxima seção.

## A seção de recursos do arquivo de manifesto

Este tópico descreve a seção de recursos do arquivo de manifesto, na qual você definirá os recursos necessários para suas personalizações. Essa seção do arquivo de manifesto começa nos recursos de palavras-chave e continua até o final do arquivo.

A seção de recursos do arquivo de manifesto especifica o AWS CloudFormation StackSets ou AWS Organizations SCPs, que o cFct implanta automaticamente por meio do pipeline de código. Você pode listarOUs, contas e regiões para implantar instâncias de pilha.

As instâncias Stack são implantadas no nível da conta em vez do nível da OU. SCPssão implantados no nível da OU. Para obter mais informações, consulte Crie suas próprias personalizações.

O modelo de exemplo a seguir descreve as possíveis entradas que estão disponíveis para a seção de recursos do arquivo de manifesto.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
    deploy_method: scp | stack_set
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
```

```
      parameter_value: [String]
  export_outputs: # list of ssm parameters to store output values
    - name: /org/member/test-ssm/app-id
      value: $[output_ApplicationId]
  regions: #list of strings
  - [String]
```

O restante deste tópico fornece definições detalhadas para as palavras-chave mostradas no exemplo de código anterior.

nome — O nome associado ao AWS CloudFormation StackSets. A string que você fornece atribui um nome mais fácil de usar para um conjunto de pilhas.

- Type: string
- Obrigatório: Sim
- Valores válidos: a-z, A-Z, 0-9 e um sublinhado (_). Qualquer outro caractere é automaticamente substituído por um sublinhado (_).

descrição — A descrição do recurso.

- Type: string
- Obrigatório: não

resource_file — Esse arquivo pode ser especificado como a localização relativa do arquivo de manifesto, um Amazon S3 URI ou URL que aponta para um AWS CloudFormation modelo ou política de controle de AWS Organizations serviço para criar recursos ou. JSON AWS CloudFormation SCPs

- Type: string
- Obrigatório: Sim

1. O exemplo a seguir mostra o`resource_file`, fornecido como um local relativo ao arquivo de recursos dentro do pacote de configuração.

   ```
   resources:
     - name: SecurityRoles
       resource_file: templates/custom-security.template
   ```

2. O exemplo a seguir mostra o arquivo de recurso fornecido como um Amazon S3. URI

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. O exemplo a seguir mostra o arquivo de recurso fornecido como um Amazon S3. HTTPS URL

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Se você fornecer um Amazon S3URL, verifique se a política de bucket permite acesso de leitura para a conta de gerenciamento da AWS Control Tower a partir da qual você está implantando o cFct. Se você fornecer um Amazon S3 HTTPSURL, verifique se o caminho usa notação de pontos. Por exemplo, `S3.us-west-1`. O cFct não oferece suporte a endpoints que contenham um traço entre o S3 e a região, como. `S3-us-west-2`

4. O exemplo a seguir mostra uma política de bucket do Amazon S3 e um ARN local onde os recursos são armazenados.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
}
```

Você substituirá o *`AccountId`* variável mostrada no exemplo com o ID da AWS conta de gerenciamento que está implantando o cFct. Para obter mais exemplos, consulte exemplos de políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

parâmetros — Especifica o nome e o valor AWS CloudFormation dos parâmetros.

- Tipo: MapList
- Obrigatório: não

A seção de parâmetros contém pares de parâmetros de chave/valor. O pseudo-modelo a seguir descreve a seção de parâmetros.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key — A chave associada ao parâmetro.
  - Type: string
  - Obrigatório: Sim (na propriedade de parâmetros)
  - Valores válidos: a-z, A-Z e 0-9
- parameter_value — O valor de entrada associado ao parâmetro.
  - Type: string
  - Obrigatório: Sim (na propriedade de parâmetros)

deploy_method — O método de implantação para implantar recursos na conta. Atualmente, deploy_method oferece suporte à implantação de recursos usando a `stack_set` opção de implantação de recursos por meio AWS CloudFormation StackSets ou a `scp` opção se você estiver implantando. SCPs

- Type: string
- Valores válidos: `stack_set` | `scp`
- Obrigatório: Sim

deployment_targets — Lista de contas ou unidades organizacionais (OUs), nas quais o cFCT implantará os AWS CloudFormation recursos, especificados como contas ou unidades_organizacionais.

> **Note**
>
> Se você quiser implantar umSCP, o destino deve ser uma OU, não uma conta.

- Tipo: Lista de seqüências de caracteres `account name` ou `account number` para indicar que esse recurso será implantado em uma determinada lista de contas ou `OU names` para indicar que esse recurso será implantado em uma determinada lista de OU.
- Obrigatório: Pelo menos uma das contas ou unidades_organizacionais
  - contas:

    Tipo: Lista de seqüências de caracteres `account name` ou `account number` para indicar que esse recurso será implantado na lista de contas especificada.
  - unidades_organizacionais:

    Tipo: Lista de seqüências de caracteres `OU names` para indicar que esse recurso será implantado em uma determinada lista de OU. Se você fornecer uma OU que não contenha contas e a propriedade de contas não for adicionada, o cFct criará apenas o conjunto de pilhas.

    > **Note**
    >
    > O ID da conta de gerenciamento da organização não é um valor permitido. O cFct não oferece suporte à implantação de instâncias de pilha na conta de gerenciamento da organização.

export_outputs — Lista de pares de nome/valor que denotam chaves de parâmetros. SSM Essas chaves de SSM parâmetros permitem que você armazene as saídas do modelo no armazenamento de SSM parâmetros. A saída é destinada à referência por outros recursos, definidos anteriormente no arquivo de manifesto.

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- Tipo: Lista de pares de chaves de nome e valor. O nome contém a `name` cadeia de caracteres de uma chave de armazenamento de SSM parâmetros e o valor contém a `value` cadeia de caracteres do parâmetro.
- Valores válidos: qualquer string ou a `$[output_`*`CfnOutput-Logical-ID`*`]` variável em que *`CfnOutput-Logical-ID`* corresponde à variável de saída do modelo. Para obter mais informações sobre a seção Saídas em um AWS CloudFormation modelo, consulte Saídas no Guia do AWS CloudFormation usuário.
- Obrigatório: não

Por exemplo, o trecho de código a seguir armazena a variável de `VPCID` saída do modelo na chave de SSM parâmetro nomeada. `/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> O nome da chave export_outputs pode conter um valor diferente de. `output` Por exemplo, se o nome for`/org/environment-name`, o valor pode ser`production`.

regiões — Lista de regiões nas quais o cFCT implantará as instâncias da AWS CloudFormation pilha.

- Tipo: qualquer lista de nomes de regiões AWS comerciais, para indicar que esse recurso será implantado em uma determinada lista de regiões. Se essa palavra-chave não existir no arquivo de manifesto, os recursos serão implantados somente na região de origem.
- Obrigatório: não

## UO raiz

O cFct suporta Root como um valor para uma unidade organizacional (OU) `organizational_units` na versão V2 do manifesto (2021-03-15).

- Se você escolher o método de implantação de`scp`, ao adicionar Root under`organizational_units`, o AWS Control Tower aplicará as políticas a todos os itens OUs abaixo da Root. Se você escolher o método de implantação de`stack_set`, ao adicionar Root

emorganizational_units, o cFct implanta os conjuntos de pilhas em todas as contas sob a Raiz que estão inscritas na Control TowerAWS, exceto na conta de gerenciamento.

- De acordo com as melhores práticas da AWS Control Tower, a conta de gerenciamento se destina apenas a gerenciar contas de membros e para fins de cobrança. Não execute cargas de trabalho de produção na conta de gerenciamento da AWS Control Tower.

  De acordo com as diretrizes de melhores práticas, a implantação do AWS Control Tower coloca a conta de gerenciamento na UO raiz, para que ela tenha acesso total e não execute recursos adicionais. Por esse motivo, a AWSControlTowerExecutionfunção não é implantada na conta de gerenciamento.
- Recomendamos que você siga essas melhores práticas para a conta de gerenciamento. Se você tiver um caso de uso específico que exija a implantação de conjuntos de pilhas na conta de gerenciamento, inclua contas como destino de implantação e especifique a conta de gerenciamento. Caso contrário, não inclua contas como destino de implantação. Você deve criar os recursos ausentes, incluindo as IAM funções necessárias, na conta de gerenciamento.

Para implantar conjuntos de pilhas na conta de gerenciamento, inclua `accounts` como destino de implantação e especifique a conta de gerenciamento. Caso contrário, não inclua contas como destino de implantação.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> O recurso Root OU é suportado somente na versão V2 do arquivo de manifesto (2021-03-15). Se você adicionar Root como UO emorganizational_units, não adicione nenhuma outraOUs.

## OU aninhada

O CFct suporta a listagem de um ou mais aninhados OUs sob a `organizational_units` palavra-chave na versão V2 do manifesto (2021-03-15).

É necessário um caminho completo (excluindo Root) para a OU aninhada, usando dois pontos como separador entre elas. OUs Para o método de implantação`scp`, o AWS Control Tower implanta SCPs a última OU no caminho de OU aninhada. Para o método de implantação`stack_set`, o AWS Control Tower implanta os conjuntos de pilhas em todas as contas na última OU no caminho aninhado da OU.

Por exemplo, considere o caminho`OUName1:OUName2:OUName3`. A última OU no caminho é`OUName3`. O cFct implanta os conjuntos SCPs to `OUName3` e stack somente em todas as contas diretamente abaixo`OUName3`.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> O recurso de OU aninhada é suportado somente na versão V2 do arquivo de manifesto (2021-03-15).

## Crie suas próprias personalizações

Para criar suas próprias personalizações, você pode modificar o `manifest.yaml` arquivo adicionando ou atualizando políticas de controle de serviços (SCPs) e AWS CloudFormation recursos. Para recursos que precisam ser implantados, você pode adicionar ou remover contas e. OUs Você pode adicionar ou modificar os modelos nas pastas do pacote, criar suas próprias pastas e referenciar os modelos ou pastas no `manifest.yaml` arquivo.

Esta seção explica as duas partes principais da criação de suas próprias personalizações:

- como configurar seu próprio pacote de configuração para políticas de controle de serviços
- como configurar seu próprio pacote de configuração para conjuntos de AWS CloudFormation pilhas

## Configurar um pacote de configuração para políticas de controle de serviços

Esta seção explica como criar um pacote de configuração para políticas de controle de serviços (SCPs). As duas partes principais desse processo são (1) preparar o arquivo de manifesto e (2) preparar sua estrutura de pastas.

Etapa 1: editar o arquivo manifest.yaml

Use o `manifest.yaml` arquivo de amostra como ponto de partida. Insira todas as configurações necessárias. Adicione `resource_file` os `deployment_targets` detalhes e.

O trecho a seguir mostra o arquivo de manifesto padrão.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

O valor de `region` é adicionado automaticamente durante a implantação. Ele deve corresponder à região em que você implantou o cFCT. Essa região deve ser igual à região da AWS Control Tower.

Para adicionar um personalizado SCP na `example-configuration` pasta do pacote zip armazenado no bucket do Amazon S3, abra o `example-manifest.yaml` arquivo e comece a editar.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
```

```
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

O trecho a seguir mostra um exemplo de um arquivo de manifesto personalizado. Você pode adicionar mais de uma política em uma única alteração.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

Etapa 2: criar uma estrutura de pastas

Você pode pular essa etapa se estiver usando um Amazon URL S3 para o arquivo de recursos e usando parâmetros com pares de chave/valor.

Você deve incluir uma SCP política em JSON formato para dar suporte ao manifesto, porque o arquivo do manifesto faz referência ao JSON arquivo. Certifique-se de que os caminhos do arquivo correspondam às informações de caminho fornecidas no arquivo manifesto.

- Um JSON arquivo de política contém o SCPs a ser implantado. OUs

O trecho a seguir mostra a estrutura de pastas do arquivo de manifesto de amostra.

```
- manifest.yaml
```

```
- policies/
   - block-s3-public.json
```

O trecho a seguir é um exemplo de um arquivo de `block-s3-public.json` política.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

## Configure um pacote de configuração para AWS CloudFormation StackSets

Esta seção explica como configurar um pacote de configuração para AWS CloudFormation StackSets. As duas partes principais desse processo são: (1) preparar o arquivo de manifesto e (2) atualizar a estrutura de pastas.

Etapa 1: editar o arquivo de manifesto existente

Adicione as novas AWS CloudFormation StackSets informações ao arquivo de manifesto que você editou anteriormente.

Apenas para análise, o trecho a seguir contém o mesmo arquivo de manifesto personalizado que foi exibido anteriormente para configurar um pacote de configuração. SCPs Agora você pode editar ainda mais esse arquivo, para incluir os detalhes sobre seus recursos.

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
```

```
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

O trecho a seguir mostra um exemplo de arquivo de manifesto editado que contém os `resources` detalhes. A ordem de `resources` determina a ordem de execução para criar `resources` dependências. Você pode editar o seguinte exemplo de arquivo de manifesto de acordo com suas necessidades comerciais.

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
```

```
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

O exemplo a seguir mostra que você pode adicionar mais de um AWS CloudFormation recurso no arquivo de manifesto.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

Etapa 2: atualizar a estrutura da pasta

Ao atualizar a estrutura de pastas, você pode incluir todos os arquivos de AWS CloudFormation modelo de suporte e arquivos SCP de políticas que estão no arquivo de manifesto. Verifique se os caminhos do arquivo correspondem ao fornecido no arquivo de manifesto.

- Um arquivo de modelo contém os AWS recursos a serem implantados OUs e as contas.
- Um arquivo de política contém os parâmetros de entrada usados no arquivo de modelo.

O exemplo a seguir mostra a estrutura de pastas do arquivo de manifesto de amostra criado na Etapa 1.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

## O auxiliar 'alfred' e os arquivos de parâmetros AWS CloudFormation

O CFct fornece um mecanismo conhecido como alfred helper para obter o valor de uma chave do SSMParameter Store definida no modelo. AWS CloudFormation Usando o auxiliar alfred, você pode usar valores armazenados no SSM Parameter Store sem atualizar o AWS CloudFormation modelo. Para obter mais informações, consulte O que é um AWS CloudFormation modelo? no Guia do AWS CloudFormation usuário.

> **Important**
>
> O ajudante alfred tem duas limitações. Os parâmetros estão disponíveis somente na região inicial da conta de gerenciamento da AWS Control Tower. Como prática recomendada, considere trabalhar com valores que não mudam de instância de pilha para instância de pilha. Quando o auxiliar 'alfred' recupera os parâmetros, ele escolhe uma instância de pilha aleatória do conjunto de pilhas que exporta a variável.

Exemplo

Suponha que você tenha dois conjuntos AWS CloudFormation de pilhas. O conjunto de pilhas 1 tem uma instância de pilha e é implantado em uma conta em uma região. Ele cria uma Amazon

VPC e sub-redes em uma zona de disponibilidade, e o `VPC ID` e `subnet ID` deve ser passado para o conjunto de pilhas 2 como valores de parâmetros. Antes que o `VPC ID` e `subnet ID` possa ser passado para o conjunto de pilhas 2, o `VPC ID` e `subnet ID` deve ser armazenado no conjunto de pilhas 1 usando. `AWS:::SSM::Parameter` Para obter mais informações, consulte `AWS:::SSM::Parameter` no Guia de Usuário AWS CloudFormation .

AWS CloudFormation conjunto de pilha 1:

No trecho a seguir, o auxiliar alfred pode obter valores para e do armazenamento `subnet ID` de parâmetros `VPC ID` e passá-los como entrada para a máquina de estado. StackSet

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation conjunto de pilhas 2:

O trecho mostra os parâmetros especificados no arquivo AWS CloudFormation stack 2. `manifest.yaml`

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation conjunto de pilhas 2.1:

O trecho mostra que você pode listar `alfred_ssm` propriedades para oferecer suporte a parâmetros do tipo. CommaDelimitedList Para obter mais informações, consulte `Parameters` no Guia de Usuário AWS CloudFormation .

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

JSONesquema para o pacote de personalização

O JSON esquema do pacote de personalização do cFct está localizado no repositório de código-fonte em. GitHub Você pode usar o esquema com muitas de suas ferramentas de desenvolvimento favoritas e pode achar que é útil para reduzir erros ao criar seu próprio `manifest.yaml` arquivo.

## Atualizações da versão do manifesto

Para obter informações sobre a versão mais recente do Customizations for AWS Control Tower (cFct), consulte o CHANGELOGarquivo.md no repositório. GitHub

Warning

A versão 2.2.0 do Customizations for AWS Control Tower (cFct) introduziu um esquema de manifesto (versão 2021-03-15) para se alinhar ao serviço relacionado. AWS APIs O esquema do manifesto permite que um único arquivo manifest.yaml gerencie os recursos compatíveis (AWS CloudFormation modelos eSCPs) por meio de fluxos de trabalho desacoplados. DevOps

É altamente recomendável que você atualize o esquema do manifesto da versão 2020-01-01 para a versão 2021-03-15 ou posterior.

O cFct continua oferecendo suporte às versões 2021-03-15 e 2020-01-01 do arquivo. `manifest.yaml` Nenhuma alteração na configuração existente é necessária. No entanto, a versão 2020-01-01 está em End of Support. Não fornecemos mais atualizações nem

adicionamos aprimoramentos à versão 2020-01-01. Os recursos de UO raiz e UO aninhada não são suportados na versão 2020-01-01.

Propriedades obsoletas na versão do manifesto 2021-03-15:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

## Etapas obrigatórias de atualização

Ao atualizar para a versão 2021-03-15 do esquema de manifesto, aqui estão as alterações que você deve fazer para atualizar seus arquivos. As próximas seções descrevem as mudanças obrigatórias e recomendadas para a transição.

### Políticas da Organizations

1. Mova o SCPs item organization_policies em novos recursos de propriedade.
2. Altere a propriedade policy_file para a nova propriedade resource_file.
3. Altere apply_to_accounts_in_ou para a nova propriedade deployment_targets. A lista de UO deve ser definida na subpropriedade organizational_units. A subpropriedade de contas não é compatível com as políticas da organização.
4. Adicione uma nova propriedade deploy_method com o valor scp.

### AWS CloudFormation recursos

1. Mova os CloudFormation recursos em cloudformation_resources em novos recursos de propriedade.
2. Altere a propriedade template_file para a nova propriedade resource_file.
3. Altere o deploy_to_ou para a nova propriedade deployment_targets. A lista de UO deve ser definida na subpropriedade organizational_units.

4. Altere o deploy_to_accounts para a nova propriedade deployment_targets. A lista de contas deve ser definida em contas de subpropriedades.
5. Altere a propriedade ssm_parameters para a nova propriedade export_outputs.

## Etapas de atualização altamente recomendadas

AWS CloudFormation parâmetros

1. Altere a propriedade parameter_file para novos parâmetros de propriedade.
2. Remova o caminho do arquivo no valor da propriedade parameter_file.
3. Copie a chave do parâmetro e o valor do parâmetro do JSON arquivo de parâmetros existente para o novo formato da propriedade parameters. Isso ajudaria você a gerenciá-los no arquivo de manifesto.

> **Note**
>
> A propriedade parameter_file é suportada na versão do manifesto 2021-03-15.

# Rede na AWS Control Tower

O AWS Control Tower fornece suporte básico para redes por meio de VPCs.

Se a configuração ou os recursos padrão da VPC do AWS Control Tower não atenderem às suas necessidades, você poderá usar outros AWS serviços para configurar sua VPC. Para obter mais informações sobre como trabalhar com VPCs e o AWS Control Tower, consulte Criação de uma infraestrutura de rede AWS multi-VPC escalável e segura.

Tópicos relacionados da

- Para obter informações sobre como o AWS Control Tower funciona quando você inscreve contas que têm VPCs existentes, consulte. Registrando contas existentes com VPCs
- Com o Account Factory, você pode provisionar contas que incluem uma VPC do AWS Control Tower ou você pode provisionar contas sem uma VPC. Para obter informações sobre como excluir a VPC da AWS Control Tower ou configurar contas da AWS Control Tower sem uma VPC, consulte. Passo a passo: Configurar o AWS Control Tower sem uma VPC
- Para obter informações sobre como alterar as configurações de conta para VPCs, consulte a documentação do Account Factory sobre como atualizar uma conta.
- Para obter mais informações sobre como trabalhar com redes e VPCs no AWS Control Tower, consulte a seção sobre redes na página de informações relacionadas deste Guia do usuário.

## VPCs e AWS regiões no AWS Control Tower

Como parte padrão da criação da conta, AWS cria uma VPC AWS padrão em todas as regiões, até mesmo nas regiões que você não governa com o AWS Control Tower. Essa VPC padrão não é a mesma que uma VPC que o AWS Control Tower cria para uma conta provisionada, mas a AWS VPC padrão em uma região não governada pode estar acessível aos usuários do IAM.

Os administradores podem ativar o controle de negação da região, para que seus usuários finais não tenham permissão para se conectar a uma VPC em uma região que é suportada pelo AWS Control Tower, mas fora de suas regiões governadas. Para configurar o controle de negação de região, acesse a página de configurações da zona de pouso e selecione Modificar configurações.

A região nega o controle bloqueia as chamadas de API para a maioria dos serviços não Regiões da AWS governados. Para obter mais informações, consulte Negar acesso a AWS com base na solicitação Região da AWS. .

> **Note**
>
> O controle de negação da região não pode impedir que os usuários do IAM se conectem a uma VPC AWS padrão em uma região onde o AWS Control Tower não é suportado.

Opcionalmente, você pode remover as VPCs AWS padrão em regiões não governadas. Para listar a VPC padrão em uma região, você pode usar um comando da CLI semelhante a este exemplo:

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

## Visão geral do AWS Control Tower e das VPCs

Aqui estão alguns fatos essenciais sobre as VPCs do AWS Control Tower:

- A VPC criada pelo AWS Control Tower quando você provisiona uma conta no Account Factory não é a mesma que a AWS VPC padrão.
- Quando a AWS Control Tower configura uma nova conta em uma AWS região compatível, a AWS Control Tower exclui automaticamente a AWS VPC padrão e configura uma nova VPC configurada pela AWS Control Tower.
- Cada conta da AWS Control Tower pode ter uma VPC criada pela AWS Control Tower. Uma conta pode ter AWS VPCs adicionais dentro do limite da conta.
- Cada VPC do AWS Control Tower tem três zonas de disponibilidade em todas as regiões, exceto na região Oeste dos EUA (Norte da Califórnia)`us-west-1`, e duas zonas de disponibilidade em. `us-west-1` Por padrão, a cada zona de disponibilidade são atribuídas uma sub-rede pública e duas sub-redes privadas. Portanto, nas regiões, exceto no Oeste dos EUA (Norte da Califórnia), cada AWS Control Tower VPC contém nove sub-redes por padrão, divididas em três zonas de disponibilidade. No Oeste dos EUA (Norte da Califórnia), seis sub-redes são divididas em duas zonas de disponibilidade.
- Cada uma das sub-redes em sua VPC do AWS Control Tower recebe um intervalo exclusivo, do mesmo tamanho.
- O número de sub-redes em uma VPC é configurável. Para obter mais informações sobre como alterar a configuração da sub-rede da VPC, consulte o tópico Fábrica de contas.
- Como os endereços IP não se sobrepõem, as seis ou nove sub-redes dentro da sua VPC do AWS Control Tower podem se comunicar entre si de forma irrestrita.

Ao trabalhar com VPCs, o AWS Control Tower não faz distinção no nível da região. Cada sub-rede é alocada do intervalo CIDR exato que você especificar. As sub-redes da VPC podem existir em qualquer região.

Observações

> **Gerencie os custos da VPC**
>
> Se você definir a configuração da VPC da Account Factory para que as sub-redes públicas sejam habilitadas ao provisionar uma nova conta, a Account Factory configura a VPC para criar um gateway NAT. Você será cobrado pelo uso da Amazon VPC.

> **Configurações de VPC e controle**
>
> Se você provisionar contas do Account Factory com as configurações de acesso à Internet da VPC ativadas, essa configuração da Account Factory substituirá o controle Proibir o acesso à Internet para uma instância da Amazon VPC gerenciada por um cliente. Para evitar a ativação do acesso à Internet para contas recém-provisionadas, você deve alterar a configuração no Account Factory. Para obter mais informações, consulte Passo a passo: Configurar o AWS Control Tower sem uma VPC.

## CIDR e emparelhamento para VPC e AWS Control Tower

Esta seção destina-se principalmente a administradores de rede. O administrador de rede da sua empresa geralmente é a pessoa que seleciona a faixa geral de CIDR para sua organização do AWS Control Tower. Depois, o administrador da rede aloca sub-redes dentro desse intervalo para fins específicos.

Quando você escolhe um intervalo CIDR para sua VPC, o AWS Control Tower valida os intervalos de endereços IP de acordo com a especificação RFC 1918. O Account Factory permite um bloco CIDR /16 de até intervalos de:

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`

- `100.64.0.0/10`(somente se o seu provedor de internet permitir o uso dessa faixa)

O delimitador `/16` permite até 65.536 endereços IP distintos.

É possível atribuir qualquer endereço IP válido dos seguintes intervalos:

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x – 172.31.x.x`
- `192.168.0.0 – 192.168.255.255` (sem IPs fora do intervalo `192.168`)

Se o intervalo que você especificar estiver fora desses, o AWS Control Tower fornecerá uma mensagem de erro.

O intervalo CIDR padrão é `172.31.0.0/16`.

Quando o AWS Control Tower cria uma VPC usando o intervalo CIDR selecionado, ele atribui o intervalo CIDR idêntico a cada VPC para cada conta que você cria dentro da unidade organizacional (OU). Devido à sobreposição padrão de endereços IP, essa implementação não permite inicialmente o emparelhamento entre nenhuma das suas VPCs do AWS Control Tower na OU.

Subredes

Dentro de cada VPC, o AWS Control Tower divide seu intervalo de CIDR especificado uniformemente em nove sub-redes (exceto no Oeste dos EUA (Norte da Califórnia), onde são seis sub-redes). Nenhuma das sub-redes se sobrepõe dentro de uma VPC. Portanto, todos eles podem se comunicar entre si, dentro da VPC.

Em resumo, por padrão, a comunicação de sub-rede dentro da VPC é irrestrita. A melhor prática para controlar a comunicação entre as sub-redes da VPC, se necessário, é configurar listas de controle de acesso com regras que definem o fluxo de tráfego permitido. Use grupos de segurança para controlar o tráfego entre instâncias específicas. Para obter mais informações sobre a configuração de grupos de segurança e firewalls no AWS Control Tower, consulte Passo a passo: Configurar grupos de segurança no AWS Control Tower com o Firewall Manager AWS.

Emparelhamento

O AWS Control Tower não restringe o emparelhamento de VPC para VPC para comunicação entre várias VPCs. No entanto, por padrão, todas as VPCs do AWS Control Tower têm o mesmo

intervalo CIDR padrão. Para oferecer suporte ao peering, você pode modificar o intervalo CIDR nas configurações do Account Factory para que os endereços IP não se sobreponham.

Se você alterar o intervalo do CIDR nas configurações do Account Factory, todas as novas contas criadas posteriormente pelo AWS Control Tower (usando o Account Factory) receberão o novo intervalo do CIDR. As contas antigas não são atualizadas. Por exemplo, você pode criar uma conta, alterar o intervalo CIDR e criar uma nova conta, e as VPCs alocadas para essas duas contas podem ser emparelhadas. O emparelhamento é possível porque os intervalos de endereços IP não são idênticos.

# Funções e permissões obrigatórias

AWSA Control Tower usa IAM funções para ajudar a gerenciar o acesso aos recursos.

Para obter informações gerais sobre funções, consulte Grupos de usuários, funções e conjuntos de permissões.

Sobre permissões

- Para obter informações sobre IAM grupos e suas permissões na AWS Control Tower, consulte grupos do IAM Identity Center para a AWS Control Tower.
- Para obter informações sobre as permissões necessárias para provisionar contas, consulte Permissões necessárias para contas.
- Para obter informações sobre as permissões do console necessárias para a AWS Control Tower, consulte Permissões necessárias para usar o console da AWS Control Tower.

Sobre funções

- Para obter informações sobre como criar uma função, incluindo permissões projetadas para acesso programático, consulte Criar funções e atribuir permissões e Funções programáticas e relações de confiança para a conta de auditoria da AWS Control Tower.
- Para obter informações sobre outras funções que a AWS Control Tower usa para gerenciar suas contas, consulte Usando políticas baseadas em identidade (IAMpolíticas) para a AWS Control Tower e as políticas gerenciadas para a AWS Control Tower.
- Para obter informações sobre AWS Control Tower e AWS Config funções, consulte AWSControl Tower ConfigRecorderRole.
- Para obter informações sobre funções que a AWS Control Tower usa para agregar AWS Config informações de suas contas, consulte Como a AWS Control Tower agrega AWS Config regras em contas OUs e contas não gerenciadas.
- Para obter informações sobre como proteger seus recursos ao atribuir funções e permissões, consulte Condições opcionais para suas relações de confiança de função, Configurar opcionalmente AWS KMS chaves e evite a falsificação de identidade entre serviços.
- Para obter informações específicas sobre o provisionamento automatizado de contas no AWS Control Tower com IAM funções, consulte Provisionamento automático de contas com funções. IAM

- Para ver a política que protege o AWS Config SNStópico, consulte O AWS Config SNSpolítica de tópicos.

# Como a AWS Control Tower trabalha com funções para criar e gerenciar contas

Em geral, as funções fazem parte do gerenciamento de identidade e acesso (IAM) em AWS. Para obter informações gerais IAM e funções em AWS, consulte o tópico de IAM funções no AWS IAMGuia do usuário .

## Funções e criação de contas

AWSA Control Tower cria a conta de um cliente ligando para `CreateAccount` API o AWS Organizations. Quando AWS Organizations cria essa conta, cria uma função dentro dessa conta, que o AWS Control Tower nomeia passando um parâmetro para API o. O nome da função é `AWSControlTowerExecution`.

AWSA Control Tower assume a `AWSControlTowerExecution` função de todas as contas criadas pelo Account Factory. Usando essa função, a AWS Control Tower define a conta como base e aplica controles obrigatórios (e quaisquer outros habilitados), o que resulta na criação de outras funções. Essas funções, por sua vez, são usadas por outros serviços, como AWS Config.

> **Note**
>
> Basear uma conta é configurar seus recursos, que incluem modelos de Account Factory, às vezes chamados de blueprints, e controles. O processo básico também configura as funções centralizadas de registro e auditoria de segurança na conta, como parte da implantação dos modelos. AWSAs linhas de base da Control Tower estão contidas nas funções que você aplica a cada conta inscrita.

Para obter mais informações sobre contas e recursos, consulteSobre Contas da AWS in AWS Control Tower.

# O AWSControlTowerExecution papel, explicado

A função `AWSControlTowerExecution` deve estar presente em todas as contas cadastradas. Ele permite que a AWS Control Tower gerencie suas contas individuais e reporte informações sobre elas às suas contas de Auditoria e Arquivo de Registros.

A `AWSControlTowerExecution` função pode ser adicionada a uma conta de várias maneiras, da seguinte forma:

- Para contas na OU de segurança (às vezes chamadas de contas principais), a AWS Control Tower cria a função no momento da configuração inicial da AWS Control Tower.
- Para uma conta Account Factory criada por meio do console AWS Control Tower, a AWS Control Tower cria essa função no momento da criação da conta.
- Para o registro de uma única conta, pedimos aos clientes que criem manualmente a função e depois inscrevam a conta no AWS Control Tower.
- Ao estender a governança para uma OU, a AWS Control Tower usa o StackSet-AWSControlTowerExecutionRole para criar a função em todas as contas dessa OU.

Objetivo da `AWSControlTowerExecution` função:

- `AWSControlTowerExecution`permite que você crie e registre contas, automaticamente, com scripts e funções Lambda.
- A função `AWSControlTowerExecution` ajuda você a configurar o registro em log de suas organizações, para que todos os logs de cada conta sejam enviados à conta de registro em log.
- `AWSControlTowerExecution`permite que você registre uma conta individual no AWS Control Tower. Primeiro, você deve adicionar a `AWSControlTowerExecution` função a essa conta. Para ver as etapas sobre como adicionar a função, consulteAdicione manualmente a IAM função necessária a uma existente Conta da AWS e inscreva-a.

Como a `AWSControlTowerExecution` função funciona comOUs:

A `AWSControlTowerExecution` função garante que os controles selecionados da AWS Control Tower se apliquem automaticamente a cada conta individual, em cada UO, em sua organização, bem como a cada nova conta que você criar na AWS Control Tower. Como resultado:

- Você pode fornecer relatórios de conformidade e segurança com mais facilidade, com base nos recursos de auditoria e registro incorporados pelos AWS controles da Control Tower.

- Suas equipes de segurança e conformidade podem verificar se todos os requisitos foram atendidos e se houve algum desvio organizacional.

Para obter mais informações sobre o desvio, consulte Detectar e resolver o desvio na AWS Control Tower.

Para resumir, a função `AWSControlTowerExecution` e sua política associada fornecem controle flexível de segurança e conformidade em toda a organização. Portanto, é menos provável que ocorram violações de segurança ou protocolo.

## Condições opcionais para sua função, relações de confiança

Você pode impor condições nas políticas de confiança de sua função para restringir as contas e os recursos que interagem com determinadas funções na AWS Control Tower. É altamente recomendável que você restrinja o acesso à `AWSControlTowerAdmin` função, pois ela permite amplas permissões de acesso.

Para ajudar a impedir que um invasor tenha acesso aos seus recursos, edite manualmente sua política de confiança do AWS Control Tower para adicionar pelo menos uma `aws:SourceArn` ou uma `aws:SourceAccount` condicional à declaração de política. Como prática recomendada de segurança, é altamente recomendável adicionar a `aws:SourceArn` condição, porque ela é mais específica do que `aws:SourceAccount` limitar o acesso a uma conta específica e a um recurso específico.

Se você não souber a totalidade ARN do recurso ou se estiver especificando vários recursos, poderá usar a `aws:SourceArn` condição com curingas (*) para as partes desconhecidas do. ARN Por exemplo, `arn:aws:controltower:*:123456789012:*` funciona se você não quiser especificar uma região.

O exemplo a seguir demonstra o uso da `aws:SourceArn` IAM condição com as políticas de confiança de sua IAM função. Adicione a condição em sua relação de confiança para a AWSControlTowerAdminfunção, porque o diretor de serviço da AWS Control Tower interage com ela.

Conforme mostrado no exemplo, a fonte ARN tem o formato: `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Substitua as sequências `${CUSTOMER_AWSACCOUNT_id}` de caracteres `${HOME_REGION}` e por sua própria região de origem e ID da conta de chamada.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

No exemplo, a Fonte ARN designada como `arn:aws:controltower:us-west-2:012345678901:*` é a única ARN autorizada a realizar a `sts:AssumeRole` ação. Em outras palavras, somente usuários que podem acessar o ID da conta`012345678901`, na `us-west-2` Região, podem realizar ações que exijam essa função específica e relação de confiança para o serviço AWS Control Tower, designado como`controltower.amazonaws.com`.

O próximo exemplo mostra `aws:SourceAccount` as `aws:SourceArn` condições aplicadas à política de confiança da função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
```

```
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

O exemplo ilustra a declaração `aws:SourceArn` condicional, com uma declaração `aws:SourceAccount` condicional adicionada. Para obter mais informações, consulte Evite a falsificação de identidade entre serviços.

Para obter informações gerais sobre políticas de permissão na AWS Control Tower, consulteGerencie o acesso aos recursos.

Recomendações:

Recomendamos que você adicione condições às funções criadas pelo AWS Control Tower, porque essas funções são assumidas diretamente por outros AWS serviços. Para obter mais informações, consulte o exemplo de AWSControlTowerAdmin, mostrado anteriormente nesta seção. Para o AWS Config função de gravador, recomendamos adicionar a `aws:SourceArn` condição, especificando o gravador ARN Config como a fonte permitida. ARN

Para funções como AWSControlTowerExecutionou outras funções programáticas que podem ser assumidas pela conta AWS Control Tower Audit em todas as contas gerenciadas, recomendamos que você adicione a `aws:PrincipalOrgID` condição à política de confiança para essas funções, o que valida que o principal que está acessando o recurso pertence a uma conta correta. AWS organização. Não adicione a declaração de `aws:SourceArn` condição, pois ela não funcionará conforme o esperado.

> **Note**
>
> Em caso de desvio, é possível que uma função da AWS Control Tower seja redefinida em determinadas circunstâncias. É recomendável que você verifique novamente as funções periodicamente, caso as tenha personalizado.

# Como a AWS Control Tower se agrega AWS Config regras em contas e contas não OUs gerenciadas

A conta de gerenciamento da AWS Control Tower cria um agregador em nível organizacional, que auxilia na detecção externa AWS Config regras, para que a AWS Control Tower não precise obter acesso a contas não gerenciadas. O console AWS Control Tower mostra quantos foram criados externamente AWS Config regras que você tem para uma determinada conta. Você pode ver detalhes sobre essas regras externas na guia External Config Rule Compliance da página de detalhes da conta.

Para criar o agregador, a AWS Control Tower adiciona uma função com as permissões necessárias para descrever uma organização e listar as contas abaixo dela. A `AWSControlTowerConfigAggregatorRoleForOrganizations` função requer a política `AWSConfigRoleForOrganizations` gerenciada e uma relação de confiança com`config.amazonaws.com`.

Aqui está a IAM política (JSONartefato) anexada à função:

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

Aqui está a relação de `AWSControlTowerConfigAggregatorRoleForOrganizations` confiança:

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
```

```
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

Para implantar essa funcionalidade na conta de gerenciamento, as seguintes permissões são adicionadas à política gerenciada`AWSControlTowerServiceRolePolicy`, que é usada pela `AWSControlTowerAdmin` função ao criar o AWS Config agregador:

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

Novos recursos criados: `AWSControlTowerConfigAggregatorRoleForOrganizations` e `aws-controltower-ConfigAggregatorForOrganizations`

Quando estiver pronto, você poderá inscrever contas individualmente ou inscrevê-las como um grupo registrando uma OU. Quando você inscreve uma conta, se você criar uma regra no AWS Config,

a AWS Control Tower detecta a nova regra. O agregador mostra o número de regras externas e fornece um link para o AWS Config console onde você pode ver os detalhes de cada regra externa da sua conta. Use as informações no AWS Config console e o console AWS Control Tower para determinar se você tem os controles apropriados habilitados para a conta.

## Funções programáticas e relações de confiança para a conta de auditoria da AWS Control Tower

Você pode entrar na conta de auditoria e assumir a função de revisar outras contas de forma programática. A conta de auditoria não permite que você faça login em outras contas manualmente.

A conta de auditoria fornece acesso programático a outras contas, por meio de algumas funções concedidas a AWS Somente funções do Lambda. Para fins de segurança, essas funções têm relações de confiança com outras funções, o que significa que as condições sob as quais as funções podem ser utilizadas são estritamente definidas.

A pilha AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` cria essas funções somente programáticas e entre contas na conta IAM de auditoria:

- aws-control tower- AdministratorExecutionRole
- aws-control tower- ReadOnlyExecutionRole

A pilha AWS Control Tower `StackSet-AWSControlTowerSecurityResources` cria essas funções somente programáticas e entre contas na conta IAM de auditoria:

- aws-control tower- AuditAdministratorRole
- aws-control tower- AuditReadOnlyRole

`ReadOnlyExecutionRole:` Observe que essa função permite que a conta de auditoria leia objetos nos buckets do Amazon S3 em toda a organização (em contraste com a `SecurityAudit` política, que permite somente o acesso aos metadados).

aws-control tower-: AdministratorExecutionRole

- Tem permissões de administrador
- Não pode ser assumido a partir do console
- Só pode ser assumido por uma função na conta de auditoria — a `aws-controltower-AuditAdministratorRole`

O artefato a seguir mostra a relação de confiança de`aws-controltower-AdministratorExecutionRole`. O número do espaço reservado `012345678901` será substituído pelo `Audit_acct_ID` número da sua conta de auditoria.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-control tower-: AuditAdministratorRole

- Pode ser assumido pelo AWS Somente serviço Lambda
- Tem permissão para realizar operações de leitura (Obter) e gravação (Colocar) em objetos do Amazon S3 com nomes que começam com o log de string

Políticas anexadas:

1. AWSLambdaExecute— AWS managed policy (política gerenciada)

2. AssumeRole-aws-controltower- AuditAdministratorRole — política embutida — Criada pela Control TowerAWS, segue o artefato.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
```

```
 }
   ]
}
```

O artefato a seguir mostra a relação de confiança para`aws-controltower-AuditAdministratorRole`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-control tower-: ReadOnlyExecutionRole

- Não pode ser assumido a partir do console
- Só pode ser assumida por outra função na conta de auditoria — a `AuditReadOnlyRole`

O artefato a seguir mostra a relação de confiança de`aws-controltower-ReadOnlyExecutionRole`. O número do espaço reservado `012345678901` será substituído pelo `Audit_acct_ID` número da sua conta de auditoria.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

aws-control tower-: AuditReadOnlyRole

- Pode ser assumido pelo AWS Somente serviço Lambda
- Tem permissão para realizar operações de leitura (Obter) e gravação (Colocar) em objetos do Amazon S3 com nomes que começam com o log de string

Políticas anexadas:

1. AWSLambdaExecute— AWS managed policy (política gerenciada)

2. AssumeRole-aws-controltower- AuditReadOnlyRole — política embutida — Criada pela Control TowerAWS, segue o artefato.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

O artefato a seguir mostra a relação de confiança para`aws-controltower-AuditAdministratorRole`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

## Provisionamento automatizado de contas com funções IAM

Para configurar as contas do Account Factory de uma forma mais automatizada, você pode criar funções Lambda na conta de gerenciamento da AWS Control Tower, que assume a AWSControlTowerExecutionfunção na conta do membro. Em seguida, usando a função, a conta de gerenciamento executa as etapas de configuração desejadas em cada conta membro.

Se você estiver provisionando contas usando funções Lambda, a identidade que executará esse trabalho deve ter a seguinte política de IAM permissões, além de. `AWSServiceCatalogEndUserFullAccess`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
```

```
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

As permissõessso:GetPeregrineStatus,, sso:ProvisionApplicationInstanceForAWSAccountsso:ProvisionApplicationProfileForA e sso:ProvisionSAMLProvide são exigidas pela AWS Control Tower Account Factory para interagir com AWS IAMCentro de identidade.

# Recursos na AWS Control Tower

- Para obter informações gerais sobre a propriedade de recursos na AWS Control Tower, consulteVisão geral do gerenciamento de permissões de acesso aos recursos da AWS Control Tower.
- Para obter informações sobre os recursos que a AWS Control Tower cria nas contas compartilhadas, consulteSobre as contas compartilhadas.
- Para obter informações sobre os recursos que a AWS Control Tower cria ao provisionar uma conta por meio do Account Factory, consulteConsiderações sobre recursos do Account Factory.
- Para ver detalhes sobre os tipos de AWS recursos definidos pela AWS Control Tower, para uso com a AWS Control Tower APIs, consulte a referência do tipo de recurso da AWS Control Tower no Guia AWS CloudFormation do Usuário.

# Como AWS as regiões funcionam com a AWS Control Tower

Atualmente, AWS o Control Tower é suportado nas seguintes AWS regiões:

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (Oregon)
- Canadá (Central)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Singapura)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europe (London)
- Europa (Estocolmo)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Tóquio)
- Europa (Paris)
- América do Sul (São Paulo)
- Oeste dos EUA (N. da Califórnia)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Osaka)
- Europa (Milão)
- África (Cidade do Cabo)
- Oriente Médio (Barém)
- Israel (Tel Aviv)
- Oriente Médio (UAE)
- Europa (Espanha)

- Ásia-Pacífico (Hyderabad)
- Europa (Zurique)
- Ásia-Pacífico (Melbourne)
- Oeste do Canadá (Calgary)

Sobre sua região de origem

Quando você cria uma landing zone, a região que você está usando para acessar o console de AWS gerenciamento se torna sua AWS região de origem para o AWS Control Tower. Durante o processo de criação, alguns recursos são provisionados na região de origem. Outros recursos, como AWS contas OUs e contas, são globais.

Depois de selecionar uma região de origem, você não poderá alterá-la.

Controles e regiões

Atualmente, todos os controles preventivos funcionam globalmente. No entanto, controles detectivos e proativos só funcionam em regiões onde o AWS Control Tower é suportado. Para obter mais informações sobre o comportamento dos controles ao ativar a AWS Control Tower em uma nova região, consulteConfigure suas regiões AWS da Control Tower.

# Configure suas regiões AWS da Control Tower

Esta seção descreve o comportamento que você pode esperar ao estender sua zona de pouso da AWS Control Tower para uma nova AWS região ou remover uma região da configuração da sua zona de pouso. Geralmente, essa ação é executada por meio da função Update do console AWS Control Tower.

> **Note**
>
> Recomendamos que você evite expandir sua zona de pouso do AWS Control Tower para AWS regiões nas quais você não exija que suas cargas de trabalho sejam executadas. Optar por não participar de uma região não impede que você implante recursos nessa região, mas esses recursos permanecerão fora da governança da AWS Control Tower.

Durante a configuração de uma nova região, a AWS Control Tower atualiza a zona de pouso, o que significa que ela define como base sua zona de pouso —

- operar ativamente em todas as regiões recém-selecionadas, e
- deixar de governar recursos em regiões não selecionadas.

As contas individuais dentro de suas unidades organizacionais (OUs) que são gerenciadas pela AWS Control Tower não são atualizadas como parte desse processo de atualização da landing zone. Portanto, você deve atualizar suas contas registrando novamente seu. OUs

Ao configurar suas regiões do AWS Control Tower, esteja ciente das seguintes recomendações e limitações:

- Selecione regiões nas quais você planeja hospedar AWS recursos ou cargas de trabalho.
- Optar por não participar de uma região não impede que você implante recursos nessa região, mas esses recursos permanecerão fora da governança da AWS Control Tower.

Quando você configura seu landing zone para novas regiões, os controles de detetive da AWS Control Tower seguem as seguintes regras:

- O que existe permanece da mesma forma. O comportamento de controle, tanto de detetive quanto de prevenção, permanece inalterado nas contas existentes, nas regiões existentes OUs e nas existentes.
- Você não pode aplicar novos controles de detetive às contas OUs existentes que não estão atualizadas. Depois de configurar sua zona de pouso da AWS Control Tower em uma nova região (atualizando sua zona de pouso), você deve atualizar as contas existentes na sua existente OUs antes de poder ativar novos controles de detetive sobre elas OUs e contas.
- Seus controles de detetive existentes começam a funcionar nas regiões recém-configuradas assim que você atualiza as contas. Quando você atualiza sua zona de pouso da AWS Control Tower para configurar novas regiões e depois atualizar uma conta, os controles de detetive que já estão habilitados na OU começarão a trabalhar nessa conta nas regiões recém-configuradas.

Configurar regiões AWS da Control Tower

1. Faça login no console do AWS Control Tower em https://console.aws.amazon.com/controltower
2. No menu de navegação do painel esquerdo, escolha Configurações da zona de pouso.
3. Na página de configurações da zona de pouso, na seção Detalhes, escolha o botão Modificar configurações no canto superior direito. Você é direcionado para o fluxo de trabalho de

atualização da zona de pouso, porque governar novas regiões ou remover regiões da governança exige que você atualize para a versão mais recente da zona de pouso.

4. Em  AWS Regiões adicionais para governança, pesquise as regiões que você deseja governar (ou parar de governar). A coluna Estado indica quais regiões você governa atualmente e quais não.
5. Marque a caixa de seleção para cada região adicional a ser governada. Desmarque a caixa de seleção de cada região da qual você está removendo a governança.

> **Note**
>
> Se você optar por não governar uma região, ainda poderá implantar recursos nessa região, mas esses recursos permanecerão fora da governança da AWS Control Tower.

6. Conclua o resto do fluxo de trabalho e escolha Atualizar landing zone.
7. Quando a configuração da landing zone for concluída, registre-se novamente OUs para atualizar as contas em suas novas regiões. Para obter mais informações, consulte Quando atualizar a AWS Control Tower OUs e as contas.

Um método alternativo de provisionar ou atualizar contas individuais após a configuração de novas regiões é usar a API estrutura do Service Catalog and the AWS CLI para atualizar as contas em um processo em lote. Para obter mais informações, consulte Provisione e atualize contas usando automação.

## Evite governança mista ao configurar regiões

É importante atualizar todas as contas em uma OU depois de estender a governança da AWS Control Tower para uma nova Região da AWS e depois de remover a governança da AWS Control Tower de uma região.

A governança mista é uma situação indesejável que pode ocorrer se os controles que regem uma OU não corresponderem totalmente aos controles que governam cada conta dentro de uma OU. A governança mista ocorre em uma OU se as contas não forem atualizadas após a AWS Control Tower estender a governança para uma nova Região da AWS ou remover a governança.

Nessa situação, determinadas contas em uma OU podem ter controles diferentes aplicados em diferentes regiões, quando comparadas a outras contas na OU ou quando comparadas à postura geral de governança da zona de destino.

Em uma OU com governança mista, se você provisionar uma nova conta, essa nova conta receberá a mesma postura (atualizada) de governança da região e da OU que a landing zone. No entanto, as contas existentes que ainda não foram atualizadas não recebem a postura atualizada de governança da região.

Em geral, a governança mista pode criar indicadores de status contraditórios ou imprecisos no console do AWS Control Tower. Por exemplo, durante a governança mista, as regiões opcionais são mostradas com o status Não governado, em registradasOUs, para contas que ainda não foram atualizadas.

> **Note**
>
> AWSA Control Tower não permite que os controles sejam ativados durante um estado de governança mista.

Comportamento dos controles durante a governança mista

- Durante a governança mista, a AWS Control Tower não pode implantar consistentemente controles baseados em AWS Config regras (ou seja, controles de detetive) em regiões que a OU já mostra como governadas, porque algumas contas na OU não foram atualizadas. Você pode receber uma mensagem `FAILED_TO_ENABLE` de erro.
- Durante a governança mista, se você estender a governança da zona de aterrissagem para uma região opcional enquanto nenhuma conta na OU ainda não tiver sido atualizada, a `EnableControl` API operação na OU falhará nos controles proativos e de detetive. Você receberá uma mensagem `FAILED_TO_ENABLE` de erro, pois contas de membros não atualizadas dentro da OU ainda não foram incluídas nessas regiões.
- Durante a governança mista, os controles que fazem parte do Security Hub Service-Managed Standard: AWS Control Tower não podem relatar a conformidade com precisão em regiões onde há uma incompatibilidade entre a configuração do landing zone e as contas que não estão atualizadas.
- A governança mista não altera o comportamento dos controles SCP baseados (controles preventivos), que se aplicam uniformemente a todas as contas em uma OU, em todas as regiões governadas.

> **Note**
>
> Governança mista não é o mesmo que deriva e não é relatada como deriva.

Para reparar a governança mista

- Escolha Atualizar conta para cada conta na OU que mostre o status Atualizar disponível na página Organizations no console.
- Escolha Re-Register OU na página Organizations, que atualiza automaticamente todas as contas na OU, caso OUs tenha menos de 1000 contas.

## Considerações sobre a ativação de regiões opcionais AWS

Embora a maioria Regiões da AWS esteja ativa por padrão para você Conta da AWS, determinadas regiões são ativadas somente quando você as seleciona manualmente. Este documento se refere a essas regiões como regiões opcionais. Por outro lado, as regiões que estão ativas por padrão, assim que a sua Conta da AWS é criada, são chamadas de regiões comerciais ou simplesmente de regiões.

O termo opt-in tem uma base histórica. Todas as Regiões da AWS introduzidas após 20 de março de 2019 são consideradas regiões optativas. As regiões opt-in têm requisitos de segurança mais altos do que as regiões comerciais no que diz respeito ao compartilhamento de IAM dados por meio de contas ativas nas regiões opt-in. Todos os dados gerenciados por meio do IAM serviço são considerados dados de identidade, incluindo usuários, grupos, funções, políticas, provedores de identidade, seus dados associados (por exemplo, certificados de assinatura X.509 ou credenciais específicas do contexto) e outras configurações no nível da conta, como política de senha e o alias da conta.

Você pode ativar regiões opcionais automaticamente durante a configuração da landing zone, selecionando-as. Sua landing zone fica ativa em todas as regiões selecionadas.

Se você optar por selecionar uma região opcional como sua região de origem do AWS Control Tower, ative-a primeiro seguindo as etapas em Habilitando uma região, quando estiver conectado ao AWS Management Console. Para trazer suas próprias contas existentes de Arquivo de Registros e Auditoria de uma região opcional, primeiro ative manualmente essa região.

As regiões AWS opcionais incluem várias regiões nas quais o AWS Control Tower está disponível:

- Região Ásia-Pacífico (Hong Kong), ap-east-1
- Região Ásia-Pacífico (Jacarta), ap-southeast-3
- Região da Europa (Milão), eu-south-1
- Região da África (Cidade do Cabo), af-south-1
- Região do Oriente Médio (Bahrein), me-south-1
- Israel (Tel Aviv), il-central-1
- Região do Oriente Médio (UAE), me-central-1
- Região da Europa (Espanha), eu-south-2
- Região Ásia-Pacífico (Hyderabad), ap-south-2
- Região da Europa (Zurique), eu-central-2
- Região Ásia-Pacífico (Melbourne), ap-southeast-4
- Região Oeste do Canadá (Calgary), ca-west-1

AWSA Control Tower tem alguns controles que funcionam de forma diferente nas regiões opcionais e nas regiões comerciais. Para obter mais informações, consulte Limitações de controle. Aqui estão algumas considerações que você deve ter em mente ao implantar cargas de trabalho em regiões opcionais.

> **Governando ou ativando?**
>
> Lembre-se de que governar uma região é uma ação que você pode selecionar no console do AWS Control Tower para que os controles possam ser aplicados na região. Ativar ou desativar uma região opcional é uma ação diferente que você pode escolher no AWS console, que abre a região em sua conta, para que você possa implantar recursos e cargas de trabalho na região.

Considerações comportamentais

- Se você optar por governar regiões de aceitação, recomendamos que você não desative (desative) nenhuma de suas regiões de aceitação governadas, pois isso pode levar à falha de suas cargas de trabalho. AWSA Control Tower não permite a desativação de uma região controlada de dentro do console da AWS Control Tower, mas certifique-se de não desativar regiões controladas de uma fonte fora da Control TowerAWS, como o AWS console de faturamento ou. AWS SDK

- Quando a AWS Control Tower estende a governança para uma região de adesão, ela é ativada (aceita) a região em todas as contas dos membros. Quando você remove uma região da governança, a AWS Control Tower não desativa (exclui) a região nas contas dos membros.
- Durante a desseleção da região, a AWS Control Tower ignora a remoção de recursos de uma região opcional se essa região tiver sido desativada manualmente para uma conta de uma fonte fora da Control TowerAWS, como o AWS console de faturamento ou. AWS SDK Recomendamos que você remova recursos das regiões que você desativou ou poderá receber cobranças inesperadas por esses recursos.
- Se sua landing zone for desativada, a AWS Control Tower limpa os recursos em todas as regiões governadas, incluindo as regiões optativas. No entanto, AWS o Control Tower não desativa as regiões opcionais. Você pode desativar as regiões opcionais como uma etapa adicional após o descomissionamento.
- Se sua região de origem for uma região opcional e se você pretende inscrever contas existentes como suas contas de Arquivo de Registro e Auditoria, você deve ativar manualmente a região de inscrição antes de selecioná-la como a região de origem do seu landing zone. Consulte Ativação de uma região.
- Se a AWS Control Tower estiver configurada com uma região opcional como sua região de origem e se você visitar o serviço AWS Control Tower a partir do AWS console em qualquer outra região, o console não o redirecionará automaticamente para a região de origem.
- O subjacente API tem limites de capacidade, o que pode aumentar a latência de alguns minutos para várias horas, dependendo do número de regiões, contas e carga de serviço. Como prática recomendada, opte apenas por aqueles em Regiões da AWS que você executará as cargas de trabalho e opte por uma região por vez.

Limitações importantes para governança e contas

- Se 16 ou mais regiões comerciais nas quais o AWS Control Tower está disponível forem governadas, incluindo regiões opcionais, o limite superior do número de contas por unidade organizacional (OU) será reduzido ao registrar uma OU. Para obter mais informações, consulte Limitações com base nos AWS serviços subjacentes.

# Configurar o controle de negação da região

AWSA Control Tower oferece dois controles de negação de região. Um controle`GRREGIONDENY`, quando ativado, se aplica a toda a landing zone. Outro controle`CTMULTISERVICEPV1`, quando

ativado, pode ser aplicado ao específico OUs especificado por você. Para obter mais informações, consulte Negar acesso AWS com base na solicitação Região da AWS e Controle de negação de região aplicado à OU.

Considerações sobre a Região negam o controle da landing zone

A Região de Negação de Controle `GRREGIONDENY`é única, porque se aplica à landing zone como um todo, e não a qualquer OU específica. Para configurar o controle de negação de região, acesse a página de configurações da zona de pouso e selecione Modificar configurações.

- Essa configuração pode ser alterada posteriormente.
- Quando ativado, esse controle se aplica a todos os cadastradosOUs.
- Esse controle não pode ser configurado individualmenteOUs.

> **Note**
>
> Antes de ativar o controle de negação de região, verifique se você não tem recursos existentes nessas regiões, pois você não terá acesso aos seus recursos depois de aplicar o controle. Enquanto o controle estiver ativado, você não poderá implantar recursos nas regiões negadas.

Quando você ativa o controle, ele se aplica a todos os registros de nível superior OUs em sua hierarquia e é herdado pela OUs parte inferior da cadeia. Quando você remove o controle, ele é removido em todas as regiões registradas OUs e não controladas na AWS Control Tower permanecem com o status Não controlado, e você pode implantar recursos em regiões fora da disponibilidade da AWS Control Tower.

> **Exceções**
>
> Você não pode negar o acesso à sua região natal. Certos AWS serviços globais, como IAM e AWS Organizations, estão isentos da Região e negam o controle. Para saber mais, consulte Negar acesso a AWS com base na solicitação Região da AWS.

- Nome completo do controle: negar acesso AWS com base na AWS região solicitada
- Descrição do controle: proíbe o acesso a operações não listadas em serviços globais e regionais fora das regiões especificadas.

- Este é um controle eletivo com orientação preventiva.

Para ver o modelo do controle de negação de regiãoSCP, consulte Negar acesso AWS com base na solicitação Região da AWS na referência do AWS Control Tower Control. O AWS Control Tower SCP é semelhante ao SCP for AWS Organizations, mas não idêntico.

Você pode determinar os pontos finais do serviço regional na página Serviços regionais.

## Considerações para que a região de nível da UE negue o controle

A principal consideração sobre o controle de negação da região no nível da OU é determinar como ele interagirá com o controle de negação da região da landing zone, se ambos estiverem ativados. Para obter mais informações, consulte Controle de negação de região aplicado à OU.

Talvez você também queira revisar Configurar o controle de negação da região.

# Provisione e gerencie contas na AWS Control Tower

Este capítulo inclui uma visão geral e procedimentos para provisionar e gerenciar contas de membros em sua landing zone da AWS Control Tower.

Também inclui uma visão geral e procedimentos para inscrever uma AWS conta existente no AWS Control Tower.

Para obter mais informações sobre contas na AWS Control Tower, consulteSobre Contas da AWS in AWS Control Tower. Para obter informações sobre como inscrever várias contas no AWS Control Tower, consulte. Registre uma unidade organizacional existente na AWS Control Tower

> **Note**
>
> Você pode realizar até cinco (5) operações relacionadas à conta simultaneamente, incluindo provisionamento, atualização e inscrição.

## Métodos de provisionamento

AWSO Control Tower fornece vários métodos para criar e atualizar contas de membros. Alguns métodos são baseados principalmente em console e alguns métodos são principalmente automatizados.

Visão geral

A forma padrão de criar contas de membros é por meio do Account Factory, um produto baseado em console que faz parte do Service Catalog. Se sua landing zone não estiver em um estado de desvio, você pode usar Create account como um método para adicionar novas contas do console, bem como Enroll account para inscrever AWS contas existentes no Control TowerAWS.

Com o Account Factory, você pode provisionar contas básicas, confiando nas configurações padrão da AWS Control Tower. Você também pode provisionar contas personalizadas que atendam aos requisitos de casos de uso especializados.

O Account Factory Customization (AFC) é uma forma de provisionar contas personalizadas a partir do console AWS Control Tower e automatiza a personalização e a implantação de suas contas. Ele permite o provisionamento automatizado baseado em console, após algumas etapas únicas de

configuração, o que elimina a necessidade de escrever scripts ou configurar pipelines. Para obter mais informações, consulte Personalize contas com Account Factory Customization (AFC).

Métodos baseados em console:

- Por meio do console Account Factory que faz parte do AWS Service Catalog, para contas básicas ou personalizadas. Revise Provisione e gerencie contas com o Account Factory para obter detalhes e instruções.
- Por meio do recurso de inscrição de conta no AWS Control Tower, se sua landing zone não estiver em um estado de deriva. Consulte Inscrever uma conta existente.
- No console do AWS Control Tower, você pode usar o Account Factory para criar, atualizar ou inscrever até cinco contas ao mesmo tempo.

Métodos automatizados:

- Código Lambda: da conta de gerenciamento da sua zona de pouso da AWS Control Tower, usando o código Lambda e as funções apropriadas. IAM Consulte Provisionamento automatizado de contas com IAM funções.
- Terraform: Da AWS Control Tower Account Factory para Terraform (AFT), que depende do Account Factory e de um GitOps modelo para permitir a automação do provisionamento e atualização de contas. Consulte Provisione contas com o AWS Control Tower Account Factory for Terraform (AFT) .
- Personalização do Account Factory no console AWS Control Tower: após as etapas de configuração, o provisionamento futuro de contas personalizadas não requer configuração adicional nem manutenção do pipeline. As contas são provisionadas por meio de um AWS Service Catalog produto chamado blueprint. Um blueprint pode usar AWS CloudFormation modelos ou modelos do Terraform.

> **Note**
>
> AWS CloudFormation Os blueprints podem implantar recursos em várias regiões. Os blueprints do Terraform podem implantar recursos somente em uma única região. Por padrão, essa é a região de origem.

# O que acontece quando a AWS Control Tower cria uma conta

Novas contas na AWS Control Tower são criadas e, em seguida, provisionadas por uma interação entre a AWS Control Tower AWS Organizations, e. AWS Service Catalog Para obter as etapas para registrar um existente Conta da AWS usando o console AWS Control Tower, consulteInscrever uma conta existente.

Nos bastidores da criação de contas

1. Você inicia a solicitação, por exemplo, na página AWS Control Tower Account Factory, diretamente do AWS Service Catalog console ou chamando o Service Catalog `ProvisionProduct`API.
2. AWS Service Catalog chama a AWS Control Tower.
3. AWSO Control Tower inicia um fluxo de trabalho, que, como primeira etapa, chama AWS Organizations `CreateAccount` API o.
4. Depois de AWS Organizations criar a conta, a AWS Control Tower conclui o processo de provisionamento aplicando esquemas e controles.
5. O Service Catalog continua pesquisando a AWS Control Tower para verificar a conclusão do processo de provisionamento.
6. Quando o fluxo de trabalho no AWS Control Tower estiver concluído, o Service Catalog finaliza o estado da conta e informa você (o solicitante) sobre o resultado.

# Permissões necessárias para contas

As permissões necessárias para cada método de provisionamento e atualização de contas são discutidas em cada seção, respectivamente. Com as permissões de grupo de usuários apropriadas, os provisionadores podem especificar linhas de base e configurações de rede padronizadas para qualquer conta em sua organização.

> **Note**
>
> Ao provisionar uma conta, o solicitante da conta sempre deve ter as permissões `CreateAccount` e as. `DescribeCreateAccountStatus` Esse conjunto de permissões faz parte da função de administrador e é concedido automaticamente quando um solicitante assume a função de administrador. Se você delegar permissão para provisionar contas, talvez seja necessário adicionar essas permissões diretamente para os solicitantes da conta.

Ao criar contas no console da AWS Control Tower com o Account Factory, você deve estar conectado a uma conta com um IAM usuário que tenha a `AWSServiceCatalogEndUserFullAccess` política ativada, junto com as permissões para usar o console da AWS Control Tower, e você não pode estar conectado como usuário raiz.

Para obter informações gerais sobre as permissões necessárias na AWS Control Tower, consulteUsando políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower. Para obter informações sobre funções e contas na AWS Control Tower, consulte Funções e contas.

> **Segurança para suas contas**
>
> Você pode encontrar orientações sobre as melhores práticas para proteger a segurança da sua conta de gerenciamento da AWS Control Tower e das contas dos membros na AWS Organizations documentação.
>
> - Melhores práticas para a conta de gerenciamento
> - Melhores práticas para contas de membros

# Sobre Contas da AWS in AWS Control Tower

An Conta da AWS é o contêiner para todos os seus recursos próprios. Esses recursos incluem as AWS Identity and Access Management (IAM) identidades aceitas pela conta, que determinam quem tem acesso a essa conta. IAMas identidades podem incluir usuários, grupos, funções e muito mais. Para obter mais informações sobre como trabalhar com usuáriosIAM, funções e políticas na AWS Control Tower, consulte Gerenciamento de identidade e acesso na AWS Control Tower.

Recursos e tempo de criação da conta

Quando a AWS Control Tower cria ou inscreve uma conta, ela implanta a configuração mínima necessária de recursos para a conta, incluindo recursos na forma de modelos de Account Factory e outros recursos em sua landing zone. Esses recursos podem incluir IAM funções, AWS CloudTrail trilhas, produtos provisionados pelo Service Catalog e usuários do IAM Identity Center. AWSA Control Tower também implanta recursos, conforme exigido pela configuração de controle, para a unidade organizacional (OU) na qual a nova conta está destinada a se tornar uma conta membro.

AWSA Control Tower orquestra a implantação desses recursos em seu nome. Pode ser necessário vários minutos por recurso para concluir a implantação, portanto, considere o tempo total antes de

criar ou inscrever uma conta. Para obter mais informações sobre como gerenciar recursos em suas contas, consulteOrientação para criar e modificar recursos da AWS Control Tower.

## Considerações sobre como trazer contas de segurança ou registro existentes

Antes de aceitar uma conta Conta da AWS como de segurança ou de registro, a AWS Control Tower verifica se há recursos que entrem em conflito com os requisitos da AWS Control Tower. Por exemplo, você pode ter um bucket de registro com o mesmo nome que o AWS Control Tower exige. Além disso, a AWS Control Tower valida que a conta pode provisionar recursos; por exemplo, garantindo que AWS Security Token Service (AWS STS) esteja habilitado, que a conta não seja suspensa e que a AWS Control Tower tenha permissão para provisionar recursos dentro da conta.

AWSO Control Tower não remove nenhum recurso existente nas contas de registro e segurança que você fornece. No entanto, se você optar por ativar o recurso de Região da AWS negação, o controle de negação de região impedirá o acesso a recursos em regiões negadas.

## Veja suas contas

A página Organização lista todas OUs as contas em sua organização, independentemente da OU ou do status de inscrição na AWS Control Tower. Você pode visualizar e inscrever contas de membros na Torre de AWS Controle — individualmente ou por grupos de UO — se cada conta atender aos pré-requisitos para inscrição.

Para ver uma conta específica na página Organização, você pode escolher Contas somente no menu suspenso no canto superior direito e, em seguida, selecionar o nome da sua conta na tabela. Como alternativa, você pode selecionar o nome da OU principal na tabela e exibir uma lista de todas as contas dessa OU na página Detalhes dessa OU.

Na página Organização e na página Detalhes da conta, você pode ver o estado da conta, que é um destes:

- Não cadastrada — A conta é membro da OU principal, mas não é totalmente gerenciada pela AWS Control Tower. Se a OU principal estiver registrada, a conta será governada pelos controles preventivos configurados para sua OU principal registrada, mas os controles de detetive da OU não se aplicam a essa conta. Se a OU principal não estiver registrada, nenhum controle se aplicará a essa conta.

- Inscrição — A conta está sendo colocada sob a governança da AWS Control Tower. Estamos alinhando a conta com a configuração de controle da OU principal. Esse processo pode exigir vários minutos por recurso da conta.
- Inscrito — A conta é governada pelos controles configurados para sua OU principal. É totalmente gerenciado pela AWS Control Tower.
- Falha na inscrição — A conta não pôde ser registrada no AWS Control Tower. Para obter mais informações, consulte Causas comuns de falha na inscrição.
- Atualização disponível — A conta tem uma atualização disponível. As contas nesse estado ainda estão inscritas, mas a conta deve ser atualizada para refletir as mudanças recentes feitas em seu ambiente. Para atualizar uma única conta, navegue até a página de detalhes da conta e selecione Atualizar conta.

  Se você tiver várias contas com esse estado em uma única OU, poderá optar por registrar novamente a OU e atualizar essas contas juntas.

## Recursos criados nas contas compartilhadas

Esta seção mostra os recursos que o AWS Control Tower cria nas contas compartilhadas quando você configura sua landing zone.

Para obter informações sobre os recursos da conta de membro, consulteConsiderações sobre recursos do Account Factory.

### Recursos da conta de gerenciamento

Quando você configura sua landing zone, os seguintes AWS recursos são criados em sua conta de gerenciamento.

| AWSserviço | Tipo de recurso | Nome do recurso |
|---|---|---|
| AWS Organizations | Contas | audit<br>log archive |
| AWS Organizations | OUs | Security<br>Sandbox |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS Organizations | Políticas de controle de serviço | aws-guardrails-* |
| AWS CloudFormation | Pilhas | AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER<br><br>AWSControlTowerBP-BASELINE-CONFIG-MASTER(na versão 2.6 e posterior) |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS CloudFormation | StackSets | AWSControlTowerBP-BASELINE-CLOUDTRAIL(Não implantado na versão 3.0 e versões posteriores)<br><br>AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later)<br><br>AWSControlTowerBP-BASELINE-CLOUDWATCH<br><br>AWSControlTowerBP-BASELINE-CONFIG<br><br>AWSControlTowerBP-BASELINE-ROLES<br><br>AWSControlTowerBP-BASELINE-SERVICE-ROLES<br><br>AWSControlTowerBP-SECURITY-TOPICS<br><br>AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED<br><br>AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED<br><br>AWSControlTowerLoggingResources |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| | | AWSControlTowerSecurityResources<br><br>AWSControlTowerExecutionRole |
| AWS Service Catalog | Produto | AWSControl Tower Account Factory |
| AWS Config | Agregador | aws-controltower-ConfigAggregatorForOrganizations |
| AWS CloudTrail | Trilha | aws-controltower-BaselineCloudTrail |
| Amazon CloudWatch | CloudWatch Registros | aws-controltower/CloudTrail Logs |
| AWS Identity and Access Management | Funções | AWSControlTowerAdmin<br><br>AWSControlTowerStackSetRole<br><br>AWSControlTowerCloudTrailRolePolicy |
| AWS Identity and Access Management | Políticas | AWSControlTowerServiceRolePolicy<br><br>AWSControlTowerAdminPolicy<br><br>AWSControlTowerCloudTrailRolePolicy<br><br>AWSControlTowerStackSetRolePolicy |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS IAM Identity Center | Grupos de diretórios | AWSAccountFactory<br>AWSAuditAccountAdmins<br>AWSControlTowerAdmins<br>AWSLogArchiveAdmins<br>AWSLogArchiveViewers<br>AWSSecurityAuditors<br>AWSSecurityAuditPowerUsers<br>AWSServiceCatalogAdmins |
| AWS IAM Identity Center | Conjuntos de permissões | AWSAdministratorAccess<br>AWSPowerUserAccess<br>AWSServiceCatalogAdminFullAccess<br>AWSServiceCatalogEndUserAccess<br>AWSReadOnlyAccess<br>AWSOrganizationsFullAccess |

> **Note**
>
> O não AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` está implantado nas versões 3.0 ou posteriores do landing zone. No entanto, ele continua existindo nas versões anteriores da zona de pouso, até que você atualize sua zona de pouso.

## Recursos da conta de arquivamento de registros

Quando você configura sua landing zone, os seguintes AWS recursos são criados em sua conta de arquivamento de registros.

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS CloudFormation | Pilhas | StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED-<br><br>StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED<br><br>StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-<br><br>StackSet-AWSControlTowerBP-BASELINE-CONFIG-<br><br>StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-<br><br>StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-<br><br>StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| | | StackSet-AWSControlTowerBP-BASELINE-ROLES-<br><br>StackSet-AWSControlTowerLoggingResources- |
| AWS Config | Regras do AWS Config | AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED<br><br>AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT |
| AWS CloudTrail | Trilhas | aws-controltower-BaselineCloudTrail |
| Amazon CloudWatch | CloudWatch Regras do evento | aws-controltower-ConfigComplianceChangeEventRule |
| Amazon CloudWatch | CloudWatch Registros | /aws/lambda/aws-controltower-NotificationForwarder |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | aws-controltower-AdministratorExecutionRole<br>aws-controltower-CloudWatchLogsRole<br>aws-controltower-ConfigRecorderRole<br>aws-controltower-ForwardSnsNotificationRole<br>aws-controltower-ReadOnlyExecutionRole<br>AWSControlTowerExecution |
| AWS Identity and Access Management | Políticas | AWSControlTowerServiceRolePolicy |
| Amazon Simple Notification Service | Tópicos | aws-controltower-SecurityNotifications |
| AWS Lambda | Aplicações | StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* |
| AWS Lambda | Funções | aws-controltower-NotificationForwarder |
| Amazon Simple Storage Service | Buckets | aws-controltower-logs-*<br>aws-controltower-s3-access-logs-* |

## Recursos da conta de auditoria

Quando você configura sua landing zone, os seguintes AWS recursos são criados em sua conta de auditoria.

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS CloudFormation | Pilhas | StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED-<br><br>StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED-<br><br>StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-<br><br>StackSet-AWSControlTowerBP-BASELINE-CONFIG-<br><br>StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-<br><br>StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-<br><br>StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| | | StackSet-AWSControlTowerBP-SECURITY-TOPICS-<br><br>StackSet-AWSControlTowerBP-BASELINE-ROLES-<br><br>StackSet-AWSControlTowerSecurityResources-* |
| AWS Config | Agregador | aws-controltower-GuardrailsComplianceAggregator |
| AWS Config | Regras do AWS Config | AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED<br><br>AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED |
| AWS CloudTrail | Trilha | aws-controltower-BaselineCloudTrail |
| Amazon CloudWatch | CloudWatch Regras do evento | aws-controltower-ConfigComplianceChangeEventRule |
| Amazon CloudWatch | CloudWatch Registros | /aws/lambda/aws-controltower-NotificationForwarder |

| AWSserviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | aws-controltower-AdministratorExecutionRole<br>aws-controltower-CloudWatchLogsRole<br>aws-controltower-ConfigRecorderRole<br>aws-controltower-ForwardSnsNotificationRole<br>aws-controltower-ReadOnlyExecutionRole<br>aws-controltower-AuditAdministratorRole<br>aws-controltower-AuditReadOnlyRole<br>AWSControlTowerExecution |
| AWS Identity and Access Management | Políticas | AWSControlTowerServiceRolePolicy |
| Amazon Simple Notification Service | Tópicos | aws-controltower-AggregateSecurityNotifications<br>aws-controltower-AllConfigNotifications<br>aws-controltower-SecurityNotifications |
| AWS Lambda | Funções | aws-controltower-NotificationForwarder |

# Sobre as contas compartilhadas

Três especiais Contas da AWS estão associados ao AWS Control Tower: a conta de gerenciamento, a conta de auditoria e a conta de arquivamento de registros. Essas contas geralmente são chamadas de contas compartilhadas ou, às vezes, de contas principais.

- Você pode selecionar nomes personalizados para as contas de auditoria e arquivamento de registros ao configurar sua landing zone. Para obter informações sobre como alterar o nome de uma conta, consulte Alteração externa de nomes de recursos da AWS Control Tower.
- Você também pode especificar uma conta existente Conta da AWS como segurança ou de registro da AWS Control Tower durante o processo inicial de configuração da landing zone. Essa opção elimina a necessidade de a AWS Control Tower criar contas novas e compartilhadas. (Essa é uma seleção única.)

Para obter mais informações sobre as contas compartilhadas e seus recursos associados, consulteRecursos criados nas contas compartilhadas.

## Conta de gerenciamento

Isso Conta da AWS lança o AWS Control Tower. Por padrão, o usuário root dessa conta e o IAM usuário ou IAM administrador dessa conta têm acesso total a todos os recursos em sua landing zone.

> **Note**
>
> Como prática recomendada, recomendamos entrar como usuário do IAM Identity Center com privilégios de administrador ao executar funções administrativas no console do AWS Control Tower, em vez de fazer login como usuário raiz ou usuário IAM administrador dessa conta.

Para obter mais informações sobre as funções e os recursos disponíveis na conta de gerenciamento, consulteRecursos criados nas contas compartilhadas.

## Conta de arquivamento de logs

A conta compartilhada do arquivo de registros é configurada automaticamente quando você cria sua landing zone.

Essa conta contém um bucket central do Amazon S3 para armazenar uma cópia de todas as contas AWS CloudTrail e os arquivos de AWS Config log de todas as outras contas em sua landing zone. Como prática recomendada, recomendamos restringir o acesso à conta de arquivamento de registros às equipes responsáveis pela conformidade e pelas investigações e às ferramentas de segurança ou auditoria relacionadas. Essa conta pode ser usada para auditorias de segurança automatizadas ou para hospedar funções personalizadas Regras do AWS Config, como Lambda, para realizar ações de remediação.

> **Política de bucket do Amazon S3**
>
> Para a versão 3.3 e posterior da zona de pouso do AWS Control Tower, as contas devem atender a uma `aws:SourceOrgID` condição para qualquer permissão de gravação em seu bucket de auditoria. Essa condição garante que CloudTrail somente registros em nome de contas dentro de sua organização possam ser gravados em seu bucket do S3; ela impede que CloudTrail registros de fora da sua organização gravem em seu bucket do AWS Control Tower S3. Para obter mais informações, consulte AWSVersão 3.3 da zona de pouso da Control Tower.

Para obter mais informações sobre as funções e os recursos disponíveis na conta de arquivamento de registros, consulte Recursos da conta de arquivamento de registros

> **Note**
>
> Esses registros não podem ser alterados. Todos os registros são armazenados para fins de investigações de auditoria e conformidade relacionadas à atividade da conta.

## Conta de auditoria

Essa conta compartilhada é configurada automaticamente quando você cria sua landing zone.

A conta de auditoria deve ser restrita às equipes de segurança e conformidade com funções de auditor (somente leitura) e administrador (acesso total) entre contas em todas as contas na landing zone. Essas funções devem ser usadas pelas equipes de segurança e conformidade para:

- Realize auditorias por meio de AWS mecanismos, como hospedar funções Lambda de AWS Config regras personalizadas.
- Execute operações de segurança automatizadas, como ações de remediação.

A conta de auditoria também recebe notificações por meio do serviço Amazon Simple Notification Service (AmazonSNS). Três categorias de notificação podem ser recebidas:

- Todos os eventos de configuração — Este tópico agrega todas as AWS Config notificações CloudTrail e notificações de todas as contas em sua landing zone.
- Notificações de segurança agregadas — Este tópico agrega todas as notificações de segurança de CloudWatch eventos específicos, eventos de mudança de status de Regras do AWS Config conformidade e GuardDuty descobertas.
- Notificações de deriva — Este tópico agrega todos os avisos de deriva descobertos em todas as contasOUs, usuários e em sua SCPs landing zone. Para obter mais informações sobre deriva, consulteDetecte e resolva desvios na AWS Control Tower.

As notificações de auditoria acionadas na conta de um membro também podem enviar alertas para um SNS tópico local da Amazon. Essa funcionalidade permite que os administradores da conta se inscrevam para receber notificações de auditoria específicas de uma conta de membro individual. Como resultado, os administradores podem resolver problemas que afetam uma conta individual e, ao mesmo tempo, agregar todas as notificações da conta à sua conta de auditoria centralizada. Para obter mais informações, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

Para obter mais informações sobre as funções e os recursos disponíveis na conta de auditoria, consulteRecursos da conta de auditoria.

Para obter mais informações sobre auditoria programática, consulte Funções programáticas e relações de confiança para a conta de auditoria da AWS Control Tower.

> **Important**
>
> O endereço de e-mail que você fornece para a conta de auditoria recebe e-mails de AWS notificação - confirmação de assinatura de todos os e-mails Região da AWS suportados pela AWS Control Tower. Para receber e-mails de conformidade em sua conta de auditoria, você deve escolher o link Confirmar assinatura em cada e-mail de cada um Região da AWS suportado pela AWS Control Tower.

## Sobre as contas dos membros

As contas de membros são as contas por meio das quais seus usuários realizam suas AWS cargas de trabalho. Essas contas de membros podem ser criadas no Account Factory, por usuários do IAM

Identity Center com privilégios de administrador no console do Service Catalog ou por métodos automatizados. Quando criadas, essas contas de membros existem em uma OU que foi criada no console da AWS Control Tower ou registrada na AWS Control Tower. Para obter mais informações, consulte estes tópicos relacionados:

- Provisione e gerencie contas com o Account Factory
- Automatize tarefas no AWS Control Tower
- AWS Terminologia e conceitos de Organizations no Guia do AWS Organizations Usuário.

Também consulte Provisione contas com o AWS Control Tower Account Factory for Terraform (AFT) .

> **Contas e controles**
>
> As contas dos membros podem ser inscritas no AWS Control Tower ou podem ser canceladas. Os controles se aplicam de forma diferente às contas inscritas e não inscritas, e os controles podem se aplicar às contas aninhadas com base na heraçaOUs.

Para obter informações sobre os recursos da conta do membro que a AWS Control Tower aloca, consulte. Considerações sobre recursos do Account Factory

## Inscrever um existente Conta da AWS

Você pode estender a governança da AWS Control Tower a um indivíduo, existente Conta da AWS quando você o inscreve em uma unidade organizacional (OU) que já é governada pela AWS Control Tower. Existem contas elegíveis em pessoas não registradas OUs que fazem parte da mesma AWS Organizations organização da AWS Control Tower OU.

> **Note**
>
> Você não pode inscrever uma conta existente para servir como sua conta de auditoria ou arquivamento de registros, exceto durante a configuração inicial do landing zone.

Configure primeiro o acesso confiável

Antes de inscrever um existente Conta da AWS na AWS Control Tower, você deve dar permissão para que a AWS Control Tower gerencie ou controle a conta. Especificamente, a AWS Control Tower exige permissão para estabelecer acesso confiável entre AWS CloudFormation e AWS Organizations em seu nome, para que AWS CloudFormation possa implantar sua pilha automaticamente nas contas da organização selecionada. Com esse acesso confiável, a `AWSControlTowerExecution` função realiza as atividades necessárias para gerenciar cada conta. É por isso que você deve adicionar essa função a cada conta antes de inscrevê-la.

Quando o acesso confiável está ativado, AWS CloudFormation pode criar, atualizar ou excluir pilhas em várias contas e Regiões da AWS com uma única operação. AWSA Control Tower conta com esse recurso de confiança para poder aplicar funções e permissões às contas existentes antes de transferi-las para uma unidade organizacional registrada e, assim, colocá-las sob controle.

Para saber mais sobre acesso confiável e AWS CloudFormation StackSets, veja AWS CloudFormationStackSetsAWS Organizationse.

## O que acontece durante a inscrição na conta

Durante o processo de inscrição, a AWS Control Tower executa as seguintes ações:

- Aplicar linhas de base à conta, que inclui a implantação destes conjuntos de pilhas:
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
  - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
  - `AWSControlTowerBP-BASELINE-CONFIG`
  - `AWSControlTowerBP-BASELINE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
  - `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

  É uma boa ideia revisar os modelos desses conjuntos de pilhas e verificar se eles não entram em conflito com suas políticas existentes.
- Identifica a conta por meio de AWS IAM Identity Center ou AWS Organizations.
- Coloca a conta na UO especificada. Certifique-se de aplicar tudo o SCPs que é aplicado na OU atual, para que sua postura de segurança permaneça consistente.
- Aplica controles obrigatórios à conta por meio dos SCPs que se aplicam à OU selecionada como um todo.

- Ativa AWS Config e configura para registrar todos os recursos na conta.
- Adiciona as AWS Config regras que aplicam os controles de detetive da AWS Control Tower à conta.

> **Trilhas em nível de contas e organização CloudTrail**
>
> Todas as contas de membros em uma OU são regidas pela AWS CloudTrail trilha da OU, inscritas ou não:
>
> - Quando você inscreve uma conta no AWS Control Tower, sua conta é governada pela AWS CloudTrail trilha da nova organização. Se você já tiver uma implantação de uma CloudTrail trilha, poderá ver cobranças duplicadas, a menos que exclua a trilha existente da conta antes de inscrevê-la na AWS Control Tower.
> - Se você mover uma conta para uma OU registrada, por exemplo, por meio do AWS Organizations console, e não continuar inscrevendo a conta no Control TowerAWS, talvez queira remover todas as trilhas restantes no nível da conta. Se você já tiver uma implantação de uma CloudTrail trilha, você incorrerá em cobranças duplicadas. CloudTrail
>
> Se você atualizar sua landing zone e optar por não receber trilhas em nível organizacional, ou se sua landing zone for anterior à versão 3.0, as trilhas em nível organizacional não se aplicarão às suas CloudTrail contas.

## Registrando contas existentes com VPCs

AWSO Control Tower lida VPCs de forma diferente quando você provisiona uma nova conta no Account Factory do que quando você inscreve uma conta existente.

- Quando você cria uma nova conta, o AWS Control Tower remove automaticamente o AWS padrão VPC e cria um novo VPC para essa conta.
- Quando você inscreve uma conta existente, a AWS Control Tower não cria uma nova VPC para essa conta.
- Quando você inscreve uma conta existente, o AWS Control Tower não remove nenhuma conta existente VPC ou AWS padrão VPC associada à conta.

> **Tip**
>
> Você pode alterar o comportamento padrão de novas contas configurando o Account Factory, para que ele não configure um VPC por padrão para contas em sua organização sob AWS Control Tower. Para obter mais informações, consulte Crie uma conta no AWS Control Tower sem uma VPC.

## Pré-requisitos para inscrição

Esses pré-requisitos são necessários antes que você possa inscrever um existente no Conta da AWS Control Tower: AWS

1. Para cadastrar uma existente Conta da AWS, a `AWSControlTowerExecution` função deve estar presente na conta que você está cadastrando. Você pode consultar Inscrever uma conta para obter detalhes e instruções.
2. Além da `AWSControlTowerExecution` função, a existente Conta da AWS que você deseja inscrever deve ter as seguintes permissões e relações de confiança estabelecidas. Caso contrário, o registro falhará.

   Permissão de função: `AdministratorAccess` (política AWS gerenciada)

   Relação de confiança da função:

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::Management Account ID:root"
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }
   ```

3. Recomendamos que a conta não tenha um gravador AWS Config de configuração ou canal de entrega. Eles podem ser excluídos ou modificados AWS CLI antes que você possa registrar uma

conta. Caso contrário, consulte Inscrever contas que tenham AWS Config recursos existentes para obter instruções sobre como você pode modificar seus recursos existentes.

4. A conta que você deseja inscrever deve existir na mesma AWS Organizations organização que a conta de gerenciamento da AWS Control Tower. A conta existente só pode ser inscrita na mesma organização da conta de gerenciamento da AWS Control Tower, em uma OU que já esteja registrada na AWS Control Tower.

Para verificar outros pré-requisitos para inscrição, consulte Getting Started with Control Tower. AWS

> **Note**
>
> Quando você inscreve uma conta na AWS Control Tower, sua conta é governada pela AWS CloudTrail trilha da organização da AWS Control Tower. Se você já tiver uma implantação de uma CloudTrail trilha, poderá ver cobranças duplicadas, a menos que exclua a trilha existente da conta antes de inscrevê-la na AWS Control Tower.

## Inscrever uma conta existente

O recurso Inscrever conta está disponível no console da AWS Control Tower, para cadastrar contas existentes de Contas da AWS forma que sejam governadas pela Control TowerAWS. Para obter mais informações, consulte Inscrever um existente Conta da AWS.

O recurso Enroll account (Registrar conta) estará disponível quando sua zona de destino não estiver em um estado de oscilação. Para ver esse recurso no console:

- Navegue até a página Organização no AWS Control Tower.
- Encontre o nome da conta que você deseja cadastrar. Para encontrá-la, escolha Somente contas no menu suspenso no canto superior direito e localize o nome da conta na tabela filtrada.
- Siga as etapas para registrar uma conta individual, conforme mostrado na Etapas para registrar uma conta seção.

> **Note**
>
> Ao inscrever um existente Conta da AWS, certifique-se de verificar o endereço de e-mail existente. Caso contrário, uma nova conta poderá ser criada.

Determinados erros podem exigir que você atualize a página e tente novamente. Se sua zona de destino estiver em estado de oscilação, talvez não seja possível usar o recurso Enroll account (Registrar conta) com êxito. Você precisará provisionar novas contas por meio do Account Factory até que seu desvio na landing zone seja resolvido.

Ao inscrever contas no console do AWS Control Tower, você deve estar conectado a uma conta com um usuário que tenha a `AWSServiceCatalogEndUserFullAccess` política ativada, junto com as permissões de acesso do administrador para usar o console da AWS Control Tower, e você não pode estar conectado como usuário raiz.

As contas que você cadastrar podem ser atualizadas por meio da fábrica de AWS Service Catalog contas da AWS Control Tower, da mesma forma que você atualizaria qualquer outra conta. Os procedimentos de atualização são fornecidos na seção Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog.

## Etapas para registrar uma conta

Depois que a AdministratorAccesspermissão (política) estiver em vigor em sua conta existente, siga estas etapas para registrar a conta:

Para inscrever uma conta individual na AWS Control Tower

- Navegue até a página AWS Control Tower Organization.
- Na página Organização, as contas que estão qualificadas para serem inscritas permitem que você selecione Inscrever-se no menu suspenso Ações na parte superior da seção. Essas contas também mostram um botão Inscrever conta quando você as visualiza na página de detalhes da conta.
- Ao escolher Inscrever conta, você verá uma página Inscrever conta, na qual será solicitado que você adicione a `AWSControlTowerExecution` função à conta. Para obter algumas instruções, consulteAdicione manualmente a IAM função necessária a uma existente Conta da AWS e inscreva-a.
- Em seguida, selecione uma OU registrada na lista suspensa. Se a conta já estiver em uma OU registrada, essa lista mostrará a OU.
- Escolha Enroll account (Registrar conta).
- Você verá um lembrete modal para adicionar a `AWSControlTowerExecution` função e confirmar a ação.
- Escolha Inscrever-se.

- AWSO Control Tower inicia o processo de inscrição e você é direcionado de volta à página de detalhes da conta.

## Causas comuns de falha na inscrição

- Para cadastrar uma conta existente, a `AWSControlTowerExecution` função deve estar presente na conta que você está cadastrando.
- Seu IAM diretor pode não ter as permissões necessárias para provisionar uma conta.
- AWS Security Token Service (AWS STS) está desativado Conta da AWS em sua região de origem ou em qualquer região suportada pela AWS Control Tower.
- Você pode estar conectado a uma conta que precisa ser adicionada ao Account Factory Portfolio em AWS Service Catalog. A conta deve ser adicionada antes que você tenha acesso ao Account Factory para que você possa criar ou inscrever uma conta na AWS Control Tower. Se o usuário ou a função apropriada não forem adicionados ao portfólio do Account Factory, você receberá uma mensagem de erro ao tentar adicionar uma conta. Para obter instruções sobre como conceder acesso aos AWS Service Catalog portfólios, consulte Conceder acesso aos usuários.
- É possível que você esteja conectado como raiz.
- A conta que você está tentando registrar pode ter AWS Config configurações residuais. Em particular, a conta pode ter um gravador de configuração ou um canal de entrega. Eles devem ser excluídos ou modificados por meio do AWS CLI antes que você possa registrar uma conta. Para ter mais informações, consulte Inscrever contas que tenham recursos existentes AWS Config e Interaja com AWS Control Tower por meio de AWS CloudShell.
- Se a conta pertencer a outra OU com uma conta de gerenciamento, incluindo outra OU AWS Control Tower, você deverá encerrar a conta em sua OU atual antes que ela possa ingressar em outra OU. Os recursos existentes devem ser removidos na OU original. Caso contrário, o registro falhará.
- O provisionamento e a inscrição da conta falharão se suas UOs de destino SCPs não permitirem que você crie todos os recursos necessários para essa conta. Por exemplo, uma OU SCP na sua unidade organizacional de destino pode bloquear a criação de recursos sem determinadas tags. Nesse caso, o provisionamento ou o registro da conta falham, porque o AWS Control Tower não suporta a marcação de recursos. Para obter ajuda, entre em contato com seu representante de conta ou AWS Support.

Para obter mais informações sobre como a AWS Control Tower trabalha com funções quando você cria novas contas ou inscreve contas existentes, consulte Funções e contas.

> **Tip**
>
> Se você não puder confirmar se um existente Conta da AWS atende aos pré-requisitos de inscrição, você pode configurar uma OU de inscrição e inscrever a conta nessa OU. Depois que a inscrição for bem-sucedida, você poderá mover a conta para a OU desejada. Se a inscrição falhar, nenhuma outra conta ou OUs será afetada pela falha.

Se você tiver dúvidas de que suas contas existentes e suas configurações sejam compatíveis com o AWS Control Tower, siga as melhores práticas recomendadas na seção a seguir.

Recomendado: é possível configurar uma abordagem em duas etapas para o registro da conta

- Primeiro, use um pacote de AWS Config conformidade para avaliar como suas contas podem ser afetadas por alguns AWS controles da Control Tower. Para determinar como a inscrição na AWS Control Tower pode afetar suas contas, consulte Estender a governança da AWS Control Tower usando pacotes de AWS Config conformidade.
- Depois disso, talvez você queira registrar a conta. Se os resultados de conformidade forem satisfatórios, o caminho de migração será mais fácil porque é possível registrar a conta sem consequências inesperadas.
- Depois de fazer sua avaliação, se você decidir configurar uma landing zone da AWS Control Tower, talvez seja necessário remover o canal de AWS Config entrega e o gravador de configuração que foram criados para sua avaliação. Então, você poderá configurar a AWS Control Tower com sucesso.

> **Note**
>
> O pacote de conformidade também funciona em situações em que as contas estão localizadas nos OUs registros da AWS Control Tower, mas as cargas de trabalho são executadas em AWS regiões que não têm suporte para a AWS Control Tower. Você pode usar o pacote de conformidade para gerenciar recursos em contas que existem em regiões onde a AWS Control Tower não está implantada.

# Se a conta não atender aos pré-requisitos

Lembre-se de que, como pré-requisito, as contas qualificadas para serem inscritas na governança da AWS Control Tower devem fazer parte da mesma organização geral. Para cumprir esse pré-requisito para o registro da conta, você pode seguir estas etapas preparatórias para mover uma conta para a mesma organização da Control Tower. AWS

Etapas preparatórias para colocar uma conta na mesma organização da AWS Control Tower

1. Retire a conta da organização existente. Você deve fornecer uma forma de pagamento separada se usar essa abordagem.
2. Convide a conta para se juntar à organização AWS Control Tower. Para obter mais informações, consulte Convidar uma AWS conta para participar da sua organização no Guia do AWS Organizations usuário.
3. Aceite o convite. A conta aparece na raiz da organização. Essa etapa move a conta para a mesma organização da AWS Control Tower SCPs e estabelece um faturamento consolidado.

> **Tip**
>
> Você pode enviar o convite para a nova organização antes que a conta saia da organização antiga. O convite estará aguardando quando a conta sair oficialmente de sua organização existente.

Etapas para cumprir os pré-requisitos restantes:

1. Crie a `AWSControlTowerExecution` função necessária.
2. Limpe o padrãoVPC. (Essa parte é opcional. AWSO Control Tower não altera seu padrão existenteVPC.)
3. Exclua ou modifique qualquer gravador AWS Config de configuração ou canal de entrega existente por meio do AWS CLI ou AWS CloudShell. Para obter mais informações, consulte Exemplos de AWS Config CLI comandos para o status do recurso e Inscrever contas que tenham recursos existentes AWS Config

Depois de concluir essas etapas preparatórias, você pode inscrever a conta no AWS Control Tower. Para obter mais informações, consulte Etapas para registrar uma conta. Essa etapa coloca a conta na governança total da AWS Control Tower.

Etapas opcionais para desprovisionar uma conta, para que ela possa ser cadastrada e manter sua pilha

1. Para manter a AWS CloudFormation pilha aplicada, exclua a instância da pilha dos conjuntos de pilhas e escolha Reter pilhas para a instância.
2. Encerre o produto provisionado pela conta no Account Factory AWS Service Catalog . (Essa etapa remove somente o produto provisionado da AWS Control Tower. Isso não exclui a conta.)
3. Configure a conta com os detalhes de cobrança necessários, conforme exigido para qualquer conta que não pertença a uma organização. Em seguida, remova a conta da organização. (Você faz isso para que a conta não conte no total da sua AWS Organizations cota.)
4. Limpe a conta se os recursos permanecerem e, em seguida, feche-a seguindo as etapas de encerramento da contaCancelar a inscrição de uma conta.
5. Se você tiver uma OU suspensa com controles definidos, poderá mover a conta para lá em vez de executar a Etapa 1.

## Exemplos de AWS Config CLI comandos para o status do recurso

Aqui estão alguns exemplos de AWS Config CLI comandos que você pode usar para determinar o status do gravador de configuração e do canal de entrega.

Comandos de exibição:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

A resposta normal é algo como `"name": "default"`

Comandos de exclusão:

- `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

## Adicione manualmente a IAM função necessária a uma existente Conta da AWS e inscreva-a

Se você já configurou sua landing zone da AWS Control Tower, pode começar a inscrever as contas da sua organização em uma OU registrada na AWS Control Tower. Se você não configurou sua landing zone, siga as etapas descritas no Guia do usuário do AWS Control Tower em Getting Started, Etapa 2. Depois que a landing zone estiver pronta, conclua as etapas a seguir para colocar as contas existentes sob a governança da AWS Control Tower manualmente.

Não deixe de revisar o Pré-requisitos para inscrição que foi mencionado anteriormente neste capítulo.

Antes de cadastrar uma conta na AWS Control Tower, você deve dar permissão à AWS Control Tower para gerenciar essa conta. Para fazer isso, você adicionará uma função que tenha acesso total à conta, conforme mostrado nas etapas a seguir. Essas etapas devem ser executadas para cada conta que você inscrever.

Para cada conta:

Etapa 1: Faça login com acesso de administrador à conta de gerenciamento da organização que atualmente contém a conta que você deseja inscrever.

Por exemplo, se você criou essa conta AWS Organizations e usa uma IAM função entre contas para fazer login, siga estas etapas:

1. Faça login na conta de gerenciamento da sua organização.
2. Acesse AWS Organizations.
3. Em Contas, selecione a conta que você deseja registrar e copie o ID da conta.
4. Abra o menu suspenso da conta na barra de navegação superior e escolha Trocar função.
5. No formulário Alternar função, preencha os seguintes campos:
    - Em Conta, insira o ID da conta que você copiou.

- Em Função, insira o nome da IAM função que permite o acesso entre contas a essa conta. O nome dessa função foi definido quando a conta foi criada. Se você não especificou um nome de função ao criar a conta, insira o nome de função padrão,`OrganizationAccountAccessRole`.

6. Selecione Switch Role (Mudar de função).
7. Agora você deve estar conectado AWS Management Console à conta de criança.
8. Ao terminar, permaneça na conta da criança durante a próxima parte do procedimento.
9. Anote o ID da conta de gerenciamento, pois você precisará inseri-lo na próxima etapa.

Etapa 2: dê permissão à AWS Control Tower para gerenciar a conta.

1. Acesse IAM.
2. Vá para Funções.
3. Selecione Criar função.
4. Quando solicitado a selecionar para qual serviço a função se destina, escolha Política de confiança personalizada.
5. Copie o exemplo de código mostrado aqui e cole-o no documento de política. Substitua a string *`ID da conta de gerenciamento`* com o ID real da conta de gerenciamento da sua conta de gerenciamento. Aqui está a política a ser colada:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
         "AWS": "arn:aws:iam::Management Account ID:root"
         },
         "Action": "sts:AssumeRole",
         "Condition": {}
      }
   ]
  }
```

6. Quando solicitado a anexar políticas, escolha AdministratorAccess.
7. Selecione Next: Tags (Próximo: tags).

8. Você pode ver uma tela opcional intitulada Adicionar tags. Pule esta tela por enquanto escolhendo Avançar:Revisão
9. Na tela Revisar, no campo Nome da função, insira`AWSControlTowerExecution`.
10. Insira uma breve descrição na caixa Descrição, como Permite acesso total à conta para inscrição.
11. Selecione Criar função.

Etapa 3: Registre a conta movendo-a para uma OU registrada e verifique a inscrição.

Depois de configurar as permissões necessárias criando a função, siga estas etapas para registrar a conta e verificar a inscrição.

1. Faça login novamente como administrador e vá para a AWS Control Tower.
2. Registre a conta.
   - Na página Organização no AWS Control Tower, selecione sua conta e escolha Inscrever-se no menu suspenso Ações no canto superior direito.
   - Siga as etapas para registrar uma conta individual, conforme mostrado na Etapas para registrar uma conta página.
3. Verifique a inscrição.
   - Em AWS Control Tower, escolha Organização no painel de navegação à esquerda.
   - Procure a conta que você inscreveu recentemente. Seu estado inicial mostrará o status de Inscrição.
   - Quando o estado muda para Inscrito, a mudança foi bem-sucedida.

Para continuar esse processo, entre em cada conta da sua organização que você deseja inscrever no AWS Control Tower. Repita as etapas de pré-requisito e as etapas de inscrição para cada conta.

## Inscrição automatizada de contas AWS Organizations

Você pode usar o método de inscrição descrito em uma postagem de blog chamada Inscrever AWS contas existentes na AWS Control Tower para inscrever suas AWS Organizations contas na AWS Control Tower com um processo programático.

O YAML modelo a seguir pode ajudá-lo a criar a função necessária em uma conta, para que ela possa ser cadastrada programaticamente.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

# Inscrever contas que tenham recursos existentes AWS Config

Este tópico fornece uma step-by-step abordagem sobre como inscrever contas que tenham AWS Config recursos existentes. Para obter exemplos de como verificar seus recursos existentes, consulteExemplos de AWS Config CLI comandos para o status do recurso.

> **Note**
>
> Se você planeja trazer AWS contas existentes para a AWS Control Tower como contas de arquivo de auditoria e log, e se essas contas tiverem AWS Config recursos existentes, você deve excluir completamente AWS Config os recursos existentes antes de poder inscrever essas contas na AWS Control Tower para essa finalidade. Para contas que não se destinam

a se tornar contas de arquivamento de auditoria e registro, você pode modificar os recursos existentes do Config.

### Exemplos de AWS Config recursos

Aqui estão alguns tipos de AWS Config recursos que sua conta já pode ter. Esses recursos podem precisar ser modificados para que você possa inscrever sua conta no AWS Control Tower.

- AWS Config gravador
- AWS Config canal de entrega
- AWS Config autorização de agregação

### Suposições

- Você implantou uma landing zone do AWS Control Tower
- Sua conta ainda não está cadastrada no AWS Control Tower.
- Sua conta tem pelo menos um AWS Config recurso preexistente em pelo menos uma das regiões do AWS Control Tower governadas pela conta de gerenciamento.
- Sua conta não é a conta de gerenciamento do AWS Control Tower.
- Sua conta não está em desvio de governança.

Para um blog que descreve uma abordagem automatizada para cadastrar contas com AWS Config recursos existentes, consulte Automatizar a inscrição de contas com AWS Config recursos existentes no AWS Control Tower. Você poderá enviar um único ticket de suporte para todas as contas que deseja inscrever, conforme descrito emEtapa 1: Entre em contato com o suporte ao cliente com um ticket para adicionar a conta à lista de permissões do AWS Control Tower, a seguir.

### Limitações

- A conta só pode ser cadastrada usando o fluxo de trabalho do AWS Control Tower para ampliar a governança.
- Se os recursos forem modificados e criarem desvios na conta, o AWS Control Tower não atualizará os recursos.
- AWS Config os recursos em regiões que não são governadas pelo AWS Control Tower não são alterados.

> **Note**
>
> Se você tentar inscrever uma conta que tenha recursos do Config existentes, sem que a conta seja adicionada à lista de permissões, o registro falhará. Depois disso, se você tentar adicionar essa mesma conta à lista de permissões, o AWS Control Tower não poderá validar se a conta foi provisionada corretamente. Você deve cancelar o provisionamento da conta do AWS Control Tower antes de solicitar a lista de permissões e depois inscrevê-la. Se você mover a conta apenas para uma OU diferente do AWS Control Tower, isso causará uma mudança na governança, o que também impede que a conta seja adicionada à lista de permissões.

Esse processo tem 5 etapas principais.

1. Adicione a conta à lista de permissões do AWS Control Tower.
2. Crie uma nova função do IAM na conta.
3. Modifique AWS Config recursos pré-existentes.
4. Crie AWS Config recursos em AWS regiões onde eles não existem.
5. Cadastre a conta no AWS Control Tower.

Antes de continuar, considere as seguintes expectativas em relação a esse processo.

- O AWS Control Tower não cria nenhum AWS Config recurso nessa conta.
- Após o cadastro, os controles do AWS Control Tower protegem automaticamente os AWS Config recursos que você criou, incluindo a nova função do IAM.
- Se alguma alteração for feita nos AWS Config recursos após a inscrição, esses recursos devem ser atualizados para se alinharem às configurações do AWS Control Tower antes que você possa reinscrever a conta.

## Etapa 1: Entre em contato com o suporte ao cliente com um ticket para adicionar a conta à lista de permissões do AWS Control Tower

Inclua essa frase na linha de assunto do seu ticket:

Inscreva contas que tenham AWS Config recursos existentes no AWS Control Tower

Inclua os seguintes detalhes no corpo do seu ingresso:

- Número da conta de gerenciamento
- Números de contas de membros que têm AWS Config recursos existentes
- Sua região de origem selecionada para a configuração do AWS Control Tower

> **Note**
>
> O tempo necessário para adicionar sua conta à lista de permissões é de 2 dias úteis.

## Etapa 2: criar uma nova função do IAM na conta do membro

1. Abra o AWS CloudFormation console da conta do membro.
2. Crie uma nova pilha usando o seguinte modelo

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. Forneça o nome da pilha como Torre CustomerCreatedConfigRecorderRoleForControl
4. Crie a stack.

> **Note**
>
> Qualquer SCPs que você criar deve excluir uma `aws-controltower-ConfigRecorderRole*` função. Não modifique as permissões que restringem a capacidade AWS Config das regras de realizar avaliações.
> Siga estas diretrizes para que você não receba um `AccessDeniedException` quando tiver SCPs que impedem a chamada `aws-controltower-ConfigRecorderRole*` do Config.

## Etapa 3: identificar as AWS regiões com recursos pré-existentes

Para cada região governada (governada pelo AWS Control Tower) na conta, identifique e anote as regiões que têm pelo menos um dos tipos de exemplo de AWS Config recursos existentes mostrados anteriormente.

## Etapa 4: identificar as AWS regiões sem AWS Config recursos

Para cada região governada (governada pela AWS Control Tower) na conta, identifique e anote as regiões nas quais não há AWS Config recursos dos tipos de exemplo mostrados anteriormente.

## Etapa 5: Modificar os recursos existentes em cada AWS região

Para essa etapa, são necessárias as seguintes informações sobre a configuração do AWS Control Tower.

- `LOGGING_ACCOUNT`- o ID da conta de registro
- `AUDIT_ACCOUNT`- o ID da conta de auditoria
- `IAM_ROLE_ARN`- o ARN da função do IAM criado na Etapa 1
- `ORGANIZATION_ID`- o ID da organização para a conta de gerenciamento
- `MEMBER_ACCOUNT_NUMBER`- a conta do membro que está sendo modificada
- `HOME_REGION`- a região de origem da configuração do AWS Control Tower.

Modifique cada recurso existente seguindo as instruções dadas nas seções 5a a 5c, a seguir.

## Etapa 5a. AWS Config recursos de gravador

Somente um AWS Config gravador pode existir por AWS região. Se houver, modifique as configurações conforme mostrado. Substitua `GLOBAL_RESOURCE_RECORDING` o item por verdadeiro em sua região natal. Substitua o item por false para outras regiões onde existe um AWS Config gravador.

- Nome: NÃO MUDE
- RoLearn: `IAM_ROLE_ARN`
  - RecordingGroup:
  - AllSupported: verdadeiro
  - IncludeGlobalResourceTypes: `GLOBAL_RESOURCE_RECORDING`
  - ResourceTypes: Vazio

Essa modificação pode ser feita por meio da AWS CLI usando o comando a seguir. Substitua `RECORDER_NAME` a string pelo nome do AWS Config gravador existente.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

## Etapa 5b. Modifique os recursos do canal de AWS Config entrega

Somente um canal AWS Config de entrega pode existir por região. Se houver outra, modifique as configurações conforme mostrado.

- Nome: NÃO MUDE
- ConfigSnapshotDeliveryProperties: TwentyFour _Horas
- S3BucketName: O nome do bucket de registro da conta de registro do AWS Control Tower

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix: ID *DA ORGANIZAÇÃO*
- SnsTopicARN: O ARN do tópico do SNS da conta de auditoria, com o seguinte formato:

```
arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
```

Essa modificação pode ser feita por meio da AWS CLI usando o comando a seguir. Substitua *DELIVERY_CHANNEL_NAME* a string pelo nome do AWS Config gravador existente.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

## Etapa 5c. Modificar AWS Config recursos de autorização de agregação

Podem existir várias autorizações de agregação por região. O AWS Control Tower exige uma autorização de agregação que especifique a conta de auditoria como a conta autorizada e tenha a região de origem da AWS Control Tower como a região autorizada. Se ele não existir, crie um novo com as seguintes configurações:

- AuthorizedAccountId: O ID da conta de auditoria
- AuthorizedAwsRegion: A região de origem da configuração do AWS Control Tower

Essa modificação pode ser feita por meio da AWS CLI usando o seguinte comando:

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

## Etapa 6: Crie recursos onde eles não existem, em regiões governadas pela AWS Control Tower

Revise o AWS CloudFormation modelo para que, na sua região de origem, o IncludeGlobalResourcesTypesparâmetro tenha o valorGLOBAL_RESOURCE_RECORDING, conforme mostrado no exemplo a seguir. Atualize também os campos obrigatórios no modelo, conforme especificado nesta seção.

Substitua `GLOBAL_RESOURCE_RECORDING` o item por verdadeiro em sua região natal. Substitua o item por false para outras regiões onde existe um AWS Config gravador.

1. Navegue até o AWS CloudFormation console da conta de gerenciamento.
2. Crie um novo StackSet com o nome CustomerCreatedConfigResourcesForControlTower.
3. Copie e atualize o seguinte modelo:

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

Atualize o modelo com os campos obrigatórios:

a. *No `BucketName` campo **`S3`**, substitua `LOGGING_ACCOUNT_ID` e `HOME_REGION`*

b. *No `KeyPrefix` campo **`S3`**, substitua o `ORGANIZATION_ID`*

c. *No campo **`SnsTopicARN`**, substitua o `AUDIT_ACCOUNT`*

   d. No AuthorizedAccountIdcampo, substitua o *AUDIT_ACCOUNT*
   e. No AuthorizedAwsRegioncampo, substitua a *HOME_REGION*
4. Durante a implantação no AWS CloudFormation console, adicione o número da conta do membro.
5. Adicione as AWS regiões que foram identificadas na Etapa 4.
6. Implante o conjunto de pilhas.

### Etapa 7: registrar a OU com o AWS Control Tower

No painel do AWS Control Tower, registre a OU.

> **Note**
>
> O fluxo de trabalho Inscrever conta não será bem-sucedido para essa tarefa. Você deve escolher Registrar OU ou Registrar OU Novamente.

## Provisione e gerencie contas com o Account Factory

Este capítulo inclui uma visão geral e procedimentos para provisionar novas contas de membros em uma landing zone da AWS Control Tower com o Account Factory.

### Permissões para configurar e provisionar contas

O AWS Control Tower Account Factory permite que administradores e usuários da nuvem provisionem contas em sua landing zone. AWS IAM Identity Center Por padrão, os usuários do IAM Identity Center que provisionam contas devem estar no `AWSAccountFactory` grupo ou no grupo de gerenciamento.

> **Note**
>
> Tenha cuidado ao trabalhar com a conta de gerenciamento, assim como você faria ao usar qualquer conta que tenha permissões em sua organização.

A conta de gerenciamento da AWS Control Tower tem uma relação de confiança com a `AWSControlTowerExecution` função, o que permite a configuração da conta a partir da conta

de gerenciamento, incluindo algumas configurações automatizadas da conta. Para obter mais informações sobre a `AWSControlTowerExecution` função, consulte Funções e contas.

> **Note**
>
> Para inscrever um existente Conta da AWS no AWS Control Tower, essa conta deve ter a `AWSControlTowerExecution` função ativada. Para obter mais informações sobre como registrar uma conta existente, consulte Inscrever um existente Conta da AWS.

Para obter mais informações sobre permissões, consulte Permissões necessárias para contas.

## Provisionar contas com AWS Service Catalog Account Factory

O procedimento a seguir descreve como criar e provisionar contas como usuário no IAM Identity Center por meio de AWS Service Catalog. Esse procedimento também é conhecido como provisionamento avançado de contas ou provisionamento manual de contas. Opcionalmente, você pode provisionar contas programaticamente, com AWS CLI ou com o AWS Control Tower Account Factory for Terraform (). AFT Talvez você consiga provisionar contas personalizadas no console se já tiver configurado blueprints personalizados. Para obter mais informações sobre personalização, consulte Personalize contas com Account Factory Customization (AFC).

Para provisionar contas individualmente no Account Factory, como usuário

1. Faça login a partir do seu portal do usuárioURL.
2. Em Seus aplicativos, escolha AWS Conta.
3. Na lista de contas, escolha o ID da conta de gerenciamento. Essa ID também pode ter um rótulo, por exemplo, (Gerenciamento).
4. AWSServiceCatalogEndUserAccessEm, escolha Console de gerenciamento. Isso abre o AWS Management Console para este usuário nesta conta.
5. Verifique se você selecionou a conta correta Região da AWS para provisionamento, que deve ser sua região da AWS Control Tower.
6. Pesquise e escolha Service Catalog para abrir o console do Service Catalog.
7. No painel de navegação, escolha Produtos.
8. Selecione AWSControl Tower Account Factory e, em seguida, escolha o botão Iniciar produto. Essa ação inicia o assistente para provisionar uma nova conta.

9. Preencha as informações e lembre-se do seguinte:

    - SSOUserEmailPode ser um novo endereço de e-mail ou o endereço de e-mail associado a um usuário existente do IAM Identity Center. Qualquer que seja sua escolha, esse usuário terá acesso administrativo à conta que você estiver provisionando.
    - AccountEmailDeve ser um endereço de e-mail que ainda não esteja associado a um Conta da AWS. Se você usou um novo endereço de e-mail em SSOUserEmail, você pode usar esse endereço de e-mail aqui.

10. Não defina TagOptionse não ative as notificações, caso contrário, a conta poderá falhar ao ser provisionada. Ao terminar, escolha Lançar produto.
11. Revise as configurações da sua conta e escolha Launch (Iniciar). Não crie um plano de recursos, caso contrário, a conta não será provisionada.
12. Sua conta agora será provisionada. Isso poderá levar alguns minutos para ser concluído. Você pode atualizar a página para atualizar as informações de status exibidas.

> **Note**
>
> Até cinco contas podem ser provisionadas por vez.

## Considerações sobre o gerenciamento de contas no Account Factory

Você pode atualizar, cancelar a inscrição e fechar contas criadas e provisionadas por meio do Account Factory. Você pode reciclar contas atualizando os parâmetros do usuário nas contas que você deseja reutilizar. Você também pode alterar a unidade organizacional (OU) de uma conta.

> **Note**
>
> Ao atualizar um produto provisionado associado a uma conta vendida pela Account Factory, se você especificar um novo endereço de e-mail de usuário, a AWS Control AWS IAM Identity Center Tower criará um novo usuário no IAM Identity Center. A conta criada anteriormente não foi removida. Para obter informações sobre como remover o endereço de e-mail do usuário anterior do IAM Identity Center do IAM Identity Center, consulte Desabilitando um usuário.

# Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog

A maneira mais fácil de atualizar uma conta cadastrada é por meio do console AWS Control Tower. Atualizações de contas individuais são úteis para resolver desvios, como. Conta-membro migrada As atualizações da conta também são necessárias como parte de uma atualização completa da landing zone.

Se você mover uma conta de uma unidade organizacional (OU) para outra, lembre-se de que os controles aplicados pela nova OU podem ser diferentes dos controles na antiga OU. Certifique-se de que os controles na nova OU atendam aos requisitos de política da conta.

Controle o comportamento quando as contas são movidas entre OUs

Quando você move uma conta entreOUs, os controles para a OU de destino são aplicados ao conta. No entanto, os controles aplicados à conta da antiga OU não são removido. O comportamento exato dos controles é específico para a implementação do controles que estão ativos na antiga OU e na OU de destino.

- Para controles implementados com AWS Config regras: Os controles da OU anterior não são removidos. Esses controles devem ser removidos manualmente.
- Para controles implementados comSCPs: Os controles SCP baseados na OU anterior são removido. Os controles SCP baseados para a OU de destino entram em vigor nessa conta.
- Para controles implementados com AWS CloudFormation ganchos: Esse comportamento depende do status dos controles na nova OU.
  - Se a OU de destino não tiver controles baseados em gancho ativos: O antigo os controles permanecem ativos para a conta movida, a menos que você os remova manualmente.
  - Se a OU de destino tiver controles de gancho ativos: Os controles antigos são removidos e os controles na OU de destino são aplicados ao conta.

## Atualize a conta no console

Para atualizar uma conta no console AWS Control Tower

1. Quando estiver conectado ao AWS Control Tower, navegue até a página Organização.
2. Na lista de contas OUs e, selecione o nome da conta que você deseja atualizar. As contas que estão disponíveis para atualização mostram o status de Atualização disponível.

3. Em seguida, você verá a página de detalhes da conta selecionada.
4. No canto superior direito, escolha Atualizar conta.

## Atualize o produto provisionado

O procedimento a seguir orienta você sobre como atualizar sua conta no Account Factory ou movê-la para uma nova OU, atualizando o produto provisionado da conta no Service Catalog.

Para atualizar uma conta do Account Factory ou alterar sua OU por meio do Service Catalog

1. Faça login no AWS Management Console e abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog/.

   > **Note**
   >
   > Você deve entrar como um usuário com permissões para provisionar novos produtos no Service Catalog (por exemplo, um usuário `AWSAccountFactory` ou `AWSServiceCatalogAdmins` grupos do IAM Identity Center).

2. No painel de navegação, escolha Provisionamento e, em seguida, escolha Produtos provisionados.
3. Para cada uma das contas de membros listadas, execute as seguintes etapas para atualizar todas as contas de membros:

   a. Selecione uma conta de membro. Você é direcionado para a página de detalhes do produto provisionado dessa conta.

   b. Na página de detalhes do produto provisionado, escolha a guia Eventos.

   c. Anote os seguintes parâmetros:

      - SSOUserEmail(Disponível nos detalhes do produto provisionado)
      - AccountEmail(Disponível nos detalhes do produto provisionado)
      - SSOUserFirstName(Disponível no IAM Identity Center)
      - SSOUSerLastName(Disponível no IAM Identity Center)
      - AccountName(Disponível no IAM Identity Center)

   d. Em Actions (Ações), escolha Update (Atualizar).

e. Escolha o botão ao lado da Version (Versão) do produto que você deseja atualizar e escolha Next (Próximo).

f. Forneça os valores dos parâmetro que foram mencionados anteriormente.

- Se você quiser manter a OU existente ManagedOrganizationalUnit, escolha a OU na qual a conta já estava.
- Se você quiser migrar a conta para uma nova OU, para ManagedOrganizationalUnit, escolha a nova OU para a conta.

Um administrador central de nuvem pode encontrar essas informações no console do AWS Control Tower, na página Organização.

g. Escolha Próximo.

h. Reveja as alterações e escolha Update (Atualizar). Esse processo pode demorar alguns minutos por conta.

## Alterar endereço de e-mail de uma conta inscrita

Para alterar o endereço de e-mail de uma conta de membro inscrito no AWS Control Tower, siga o procedimento nesta seção.

> **Note**
>
> O procedimento a seguir não permite que você altere o endereço de e-mail de uma conta de gerenciamento, conta de arquivamento de registros ou conta de auditoria. Para obter mais informações sobre isso, consulte Como altero o endereço de e-mail associado à minha AWS conta? ou entre em contato com AWS o Support.

Para alterar o endereço de e-mail de uma conta criada pela AWS Control Tower

1. Recupere a senha do usuário root da conta. Você pode seguir as etapas no artigo Como faço para recuperar uma AWS senha perdida ou esquecida?
2. Faça login na conta com a senha do usuário root.
3. Altere o endereço de e-mail como faria com qualquer outro Conta da AWS e aguarde até que a alteração seja refletida AWS Organizations. Você pode enfrentar um atraso enquanto a alteração do endereço de e-mail termina de ser atualizada.

4. Atualize o produto provisionado no Service Catalog usando o endereço de e-mail que pertencia anteriormente à conta. O processo de atualização do produto provisionado inclui a associação do novo endereço de e-mail ao produto provisionado. Dessa forma, a alteração do endereço de e-mail entra em vigor na AWS Control Tower. Use o novo endereço de e-mail para atualizações de produtos provisionados posteriormente.

Para alterar a senha ou o endereço de e-mail de uma conta de membro que você criou AWS Organizations, consulte Como acessar uma conta de membro como usuário root no Guia do AWS Organizations usuário.

Como alternativa, você pode atualizar o endereço de e-mail de uma conta Account Factory ou de outra conta membro no AWS Organizations console sem fazer login como usuário root. Para obter mais informações, consulte Atualização do endereço de e-mail do usuário raiz para uma conta de membro AWS Organizations no Guia AWS Organizations do usuário.

## Alterar o nome de uma conta inscrita

Siga o procedimento nesta seção para alterar o nome de uma conta registrada da AWS Control Tower.

> **Note**
>
> Para alterar o nome de uma conta de AWS administrador, você deve ter permissões de administrador e estar logado como usuário raiz da conta.

Para alterar o nome de uma conta criada pela AWS Control Tower

1. Recupere a senha raiz da conta. Você pode seguir as etapas descritas neste artigo, Como faço para recuperar uma AWS senha perdida ou esquecida?
2. Faça login na conta com a senha raiz.
3. No AWS Billing console, navegue até a página de configurações da conta.
4. Altere o nome nas configurações da conta, como você faria com qualquer outro Conta da AWS.
5. AWSO Control Tower se atualiza automaticamente para refletir a mudança de nome. Essa atualização não será refletida no produto provisionado em. AWS Service Catalog

# Defina as configurações do Account Factory com a Amazon Virtual Private Cloud

O Account Factory permite que você crie linhas de base e opções de configuração pré-aprovadas para contas em sua organização. Você pode configurar e provisionar novas contas por meio do AWS Service Catalog.

Na página Account Factory, você pode ver uma lista de unidades organizacionais (OUs) e seu status na lista de permissões. Por padrão, todas OUs estão na lista de permissões, o que significa que as contas podem ser provisionadas sob elas. Você pode desativar alguns OUs para provisionamento de contas por meio de. AWS Service Catalog

Você pode ver as opções de VPC configuração da Amazon disponíveis para seus usuários finais quando eles provisionam novas contas.

Para definir as VPC configurações da Amazon em Account Factory

1. Como administrador central da nuvem, faça login no console do AWS Control Tower com permissões de administrador na conta de gerenciamento.
2. No lado esquerdo do painel, selecione Account Factory para navegar até a página de configuração de rede Account Factory. Lá é possível ver as configurações de rede padrão exibidas. Para editar, selecione Editar e veja a versão editável das configurações de rede do Account Factory.
3. Você pode modificar cada campo das configurações padrão conforme necessário. Escolha as opções de VPC configuração que você gostaria de estabelecer para todas as novas contas do Account Factory que seus usuários finais possam criar e insira suas configurações nos campos.

- Escolha desativado ou ativado para criar uma sub-rede pública na AmazonVPC. Por padrão, a sub-rede com acesso à Internet não é permitida.

> **Note**
>
> Se você definir a VPC configuração de fábrica da conta para que as sub-redes públicas sejam habilitadas ao provisionar uma nova conta, a fábrica da conta configura a Amazon VPC para criar um Gateway. NAT Você será cobrado pelo seu uso pela AmazonVPC. Consulte VPCPreços para obter mais informações.

- Escolha o número máximo de sub-redes privadas na Amazon na VPC lista. Por padrão, 1 está selecionado. O número máximo de sub-redes privadas permitido é 2 por zona de disponibilidade.
- Insira o intervalo de endereços IP para criar sua contaVPCs. O valor deve estar na forma de um bloco de roteamento entre domínios (CIDR) sem classe (por exemplo, o padrão é). `172.31.0.0/16` Esse CIDR bloco fornece o intervalo geral de endereços IP de sub-rede VPC que o Account Factory cria para sua conta. Dentro do seuVPC, as sub-redes são atribuídas automaticamente a partir do intervalo que você especifica e têm o mesmo tamanho. Por padrão, as sub-redes dentro da sua VPC não se sobrepõem. No entanto, os intervalos de endereços IP VPCs da sub-rede em todas as suas contas provisionadas podem se sobrepor.
- Escolha uma região ou todas as regiões para criar uma VPC quando uma conta for provisionada. Por padrão, todas as regiões disponíveis estão selecionadas.
- Na lista, escolha o número de zonas de disponibilidade para configurar sub-redes em cada uma. VPC O número padrão e recomendado é 3.
- Escolha Salvar.

Você pode configurar essas opções de configuração para criar novas contas que não incluam umaVPC. Veja a demonstração.

## Cancelar a inscrição de uma conta

Se você criou uma conta no Account Factory ou inscreveu uma Conta da AWS e não quer mais que a conta seja gerenciada pela AWS Control Tower em uma landing zone, você pode cancelar o registro da conta no console da AWS Control Tower.

Quando você cancela o registro de uma conta da AWS Control Tower, todos os recursos provisionados pela Control Tower AWS são removidos, incluindo todos os blueprints. A conta é movida de qualquer UO da AWS Control Tower para a área raiz. A conta não faz mais parte de uma OU registrada e não está mais sujeita à AWS Control TowerSCPs. Você pode fechar a conta por meio de AWS Organizations.

O cancelamento da inscrição de uma conta também pode ser feito no console do Service Catalog por um usuário do IAM Identity Center no `AWSAccountFactory` grupo, encerrando o Provisioned Product. Para obter mais informações sobre usuários ou grupos do IAM Identity Center, consulte Gerenciar usuários e acesso por meio de AWS IAM Identity Center. O procedimento a seguir descreve como cancelar a inscrição de uma conta membro no Service Catalog.

Para cancelar a inscrição de uma conta inscrita

1. Abra o console do Service Catalog em seu navegador da web emhttps://console.aws.amazon.com/servicecatalog.
2. No painel de navegação esquerdo, escolha Lista de produtos provisionados.
3. Na lista de contas provisionadas, escolha o nome da conta que você deseja que a AWS Control Tower não gerencie mais.
4. Na página Provisioned product details (Detalhes do produto provisionado), no menu Actions (Ações), escolha Terminate (Encerrar).
5. Na caixa de diálogo exibida, escolha Terminate (Encerrar).

> **Important**
>
> A palavra encerrar é específica do Service Catalog. Quando você encerra uma conta no Service Catalog Account Factory, a conta não é fechada. Essa ação remove a conta de sua OU e de sua landing zone.

6. Quando a conta é cancelada, seu status muda para Não cadastrada.
7. Se você não precisar mais da conta, feche-a. Para obter mais informações sobre o fechamento de AWS contas, consulte Fechar uma conta no Guia AWS Billing do usuário

Quando você cancela o registro de uma conta personalizada, a AWS Control Tower remove os recursos que o blueprint implantou, bem como quaisquer outros recursos que a Control Tower AWS criou na conta. Depois de cancelar a inscrição da conta, você pode encerrar a conta por meio de. AWS Organizations

> **Note**
>
> Uma conta não inscrita não é fechada nem excluída. Quando a conta for cancelada, o usuário do IAM Identity Center que você selecionou ao criar a conta no Account Factory ainda tem acesso administrativo à conta. Se você não quiser que esse usuário tenha acesso administrativo, altere essa configuração no IAM Identity Center atualizando a conta no Account Factory e alterando o endereço de e-mail do usuário do IAM Identity Center da conta. Para obter mais informações, consulte Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog.

### Demonstração em vídeo

Este vídeo (3:25) descreve como remover uma conta do AWS Control Tower, obter acesso root à conta e, finalmente, fechar o. Conta da AWS Você também pode fechar uma conta com um AWS Organizations API. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Passo a passo em vídeo do fechamento de uma conta no AWS Control Tower.

Você pode ver uma lista de AWS YouTube vídeos que explicam tarefas comuns na AWS Control Tower.

## Fechar uma conta criada no Account Factory

As contas criadas no Account Factory são Contas da AWS. Para obter informações sobre o fechamento Contas da AWS, consulte Fechar uma AWS conta no Guia de referência de gerenciamento de contas.

> **Note**
>
> Fechar uma conta não Conta da AWS é o mesmo que cancelar a inscrição de uma conta na Torre de AWS Controle — essas são ações separadas. Você deve cancelar o registro da conta antes de fechá-la.

### Feche uma conta de membro do AWS Control Tower por meio de AWS Organizations

Você pode fechar suas contas de membros do AWS Control Tower a partir da conta de gerenciamento da sua organização sem a necessidade de entrar em cada conta de membro individualmente com credenciais raiz, por meio de AWS Organizations. No entanto, você não pode fechar sua conta de gerenciamento dessa forma.

Quando você liga para o AWS Organizations CloseAccount APIou feche uma conta no AWS Organizations console, a conta do membro fica isolada por 90 dias, como qualquer outra Conta da AWS . A conta mostra o status Suspenso na AWS Control Tower AWS Organizations e. Se você tentar trabalhar com a conta durante esses 90 dias, a AWS Control Tower exibirá uma mensagem de erro.

Antes do vencimento dos 90 dias, você pode restaurar a conta do membro, como você pode fazer com qualquer outra Conta da AWS. Após esse período de 90 dias, os registros da conta são removidos.

Recomendamos, como prática recomendada, cancelar a inscrição de uma conta de membro antes de fechar essa conta. Se você fechar uma conta de membro sem antes desgerenciá-la, o AWS Control Tower mostrará o status da conta como Suspensa, mas também como Inscrita. Como resultado, se você tentar registrar novamente a OU da conta durante esse período de 90 dias, o AWS Control Tower produzirá uma mensagem de erro. A conta suspensa basicamente bloqueia as ações de novo registro com uma falha na pré-verificação. Se você remover a conta da OU, poderá registrá-la novamente, mas AWS poderá gerar um erro em relação à falta de um método de pagamento para a conta. Para contornar essa restrição, crie outra OU e mova a conta para essa OU antes de tentar se registrar novamente. Recomendamos que essa OU seja chamada de OU suspensa.

> **Note**
>
> Se você não cancelar o registro da conta antes de fechá-la, deverá excluir o produto provisionado da conta AWS Service Catalog após o término desses 90 dias.

Para obter mais informações, consulte a AWS Organizations documentação sobre o CloseAccount API.

## Considerações sobre recursos do Account Factory

Quando uma conta é provisionada com o Account Factory, os seguintes AWS recursos são criados na conta.

| AWS serviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS CloudFormation | Pilhas | StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-*<br><br>StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* |

| AWS serviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| | | StackSet-AWSControlTowerBP-BASELINE-CONFIG-*<br><br>StackSet-AWSControlTowerBP-BASELINE-ROLES-*<br><br>StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-* |
| AWS CloudTrail | Trilha | aws-controltower-BaselineCloudTrail |
| Amazon CloudWatch | CloudWatch Regras do evento | aws-controltower-ConfigComplianceChangeEventRule |
| Amazon CloudWatch | CloudWatch Registros | aws-controltower/CloudTrailLogs<br><br>/aws/lambda/aws-controltower-NotificationForwarder |

| AWS serviço | Tipo de recurso | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | aws-controltower-AdministratorExecutionRole<br>aws-controltower-CloudWatchLogsRole<br>aws-controltower-ConfigRecorderRole<br>aws-controltower-ForwardSnsNotificationRole<br>aws-controltower-ReadOnlyExecutionRole<br>AWSControlTowerExecution |
| AWS Identity and Access Management | Políticas | AWSControlTowerServiceRolePolicy |
| Amazon Simple Notification Service | Tópicos | aws-controltower-SecurityNotifications |
| AWS Lambda | Aplicações | StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* |
| AWS Lambda | Funções | aws-controltower-NotificationForwarder |

# Personalize contas com Account Factory Customization (AFC)

O AWS Control Tower permite que você personalize os novos e os existentes Contas da AWS ao provisionar seus recursos a partir do console do AWS Control Tower. Depois de configurar a personalização de fábrica da conta, o AWS Control Tower automatiza esse processo para provisionamento futuro, para que você não precise manter nenhum pipeline. Contas personalizadas estão disponíveis para uso imediatamente após o provisionamento dos recursos.

Suas contas personalizadas são provisionadas na fábrica de contas, por meio de AWS CloudFormation modelos ou com o Terraform. Você definirá um modelo que serve como plano de conta personalizado. Seu blueprint descreve os recursos e configurações específicos que você precisa quando uma conta é provisionada. Planos predefinidos, criados e gerenciados por AWS parceiros, também estão disponíveis. Para obter mais informações sobre esquemas gerenciados por parceiros, consulte a Biblioteca de conceitos AWS Service Catalog básicos.

> **Note**
>
> O AWS Control Tower contém controles proativos, que monitoram AWS CloudFormation recursos na AWS Control Tower. Opcionalmente, você pode ativar esses controles na sua landing zone. Quando você aplica controles proativos, eles verificam se os recursos que você está prestes a implantar em suas contas estão em conformidade com as políticas e procedimentos da sua organização. Para obter mais informações sobre controles proativos, consulte Controles proativos.

Os planos da sua conta são armazenados em uma Conta da AWS, que, para nossos propósitos, é chamada de conta hub. Os blueprints são armazenados na forma de um produto Service Catalog. Chamamos esse produto de modelo, para diferenciá-lo de qualquer outro produto do Service Catalog. Para saber mais sobre como criar produtos do Service Catalog, consulte Criação de produtos no Guia do AWS Service Catalog Administrador.

Aplique esquemas às contas existentes

Você também pode aplicar esquemas personalizados às contas existentes seguindo as etapas de atualização da conta no console do AWS Control Tower. Para obter detalhes, consulte Atualize a conta no console.

> **Antes de começar**
>
> Antes de começar a criar contas personalizadas com o AWS Control Tower Account Factory, você deve ter um ambiente de landing zone da AWS Control Tower implantado e uma unidade organizacional (OU) registrada na AWS Control Tower, onde suas contas recém-criadas serão colocadas.

Para obter mais informações sobre como trabalhar com a AFC, consulte Automatizar a personalização da conta usando a personalização da Account Factory no AWS Control Tower.

Preparação para personalização

- Você pode criar uma nova conta para servir como conta central ou usar uma existente Conta da AWS. É altamente recomendável que você não use a conta de gerenciamento do AWS Control Tower como sua conta do Blueprint Hub.
- Se você planeja se inscrever Contas da AWS no AWS Control Tower e personalizá-las, você deve primeiro adicionar a `AWSControlTowerExecution` função a essas contas, como faria com qualquer outra conta que você esteja inscrevendo no AWS Control Tower.
- Se você planeja usar planos de parceiros que tenham requisitos de assinatura do Marketplace, você deve configurá-los na sua conta de gerenciamento da AWS Control Tower antes de implantar os planos de parceiros como esquemas de personalização de fábrica de contas.

Tópicos



## Configurar para personalização

As próximas seções fornecem etapas para configurar o Account Factory para o processo de personalização. Recomendamos que você configure o administrador delegado para a conta do hub antes de iniciar essas etapas.

Resumo

- Etapa 1. Crie a função necessária. Crie uma função do IAM que conceda permissão para que o AWS Control Tower tenha acesso à conta (hub), onde os produtos do Service Catalog, também chamados de blueprints, são armazenados.
- Etapa 2. Crie o AWS Service Catalog produto. Crie o AWS Service Catalog produto (também chamado de “produto modelo”) que você precisará para definir a base da conta personalizada.
- Etapa 3. Revise seu plano personalizado. Inspecione o AWS Service Catalog produto (blueprint) que você criou.
- Etapa 4. Ligue para seu blueprint para criar uma conta personalizada. Insira as informações do modelo do produto e as informações da função nos campos apropriados no Account Factory, no console do AWS Control Tower, ao criar a conta.

## Etapa 1. Crie a função necessária

Antes de começar a personalizar contas, você deve configurar uma função que contenha uma relação de confiança entre o AWS Control Tower e sua conta do hub. Quando assumida, a função concede à AWS Control Tower acesso para administrar a conta do hub. A função deve ser nomeada AWSControlTowerBlueprintAccess.

O AWS Control Tower assume essa função para criar um recurso de portfólio em seu nome e AWS Service Catalog, em seguida, adicionar seu plano como um produto do Service Catalog a esse portfólio e, em seguida, compartilhar esse portfólio e seu plano com sua conta membro durante o provisionamento da conta.

Você criará a `AWSControlTowerBlueprintAccess` função, conforme explicado nas seções a seguir.

Navegue até o console do IAM para configurar a função necessária.

Para configurar a função em uma conta cadastrada do AWS Control Tower

1. Federe ou faça login como principal na conta de gerenciamento do AWS Control Tower.
2. Do diretor federado na conta de gerenciamento, assuma ou troque as funções para a `AWSControlTowerExecution` função na conta inscrita do AWS Control Tower que você selecionou para servir como a conta do hub do blueprint.

3. A partir da `AWSControlTowerExecution` função na conta cadastrada do AWS Control Tower, crie a `AWSControlTowerBlueprintAccess` função com permissões e relações de confiança adequadas.

> **Note**
>
> Para cumprir as diretrizes de AWS melhores práticas, é importante que você saia da `AWSControlTowerExecution` função imediatamente após criá-la. `AWSControlTowerBlueprintAccess`
> Para evitar alterações não intencionais nos recursos, a `AWSControlTowerExecution` função deve ser usada somente pelo AWS Control Tower.

Se sua conta do Blueprint Hub não estiver inscrita no AWS Control Tower, a `AWSControlTowerExecution` função não existirá na conta e não há necessidade de assumi-la antes de continuar com a configuração da `AWSControlTowerBlueprintAccess` função.

Para configurar a função em uma conta de membro não inscrito

1. Federe ou faça login como principal na conta que você deseja designar como conta central, por meio de seu método preferido.
2. Quando estiver conectado como principal na conta, crie a `AWSControlTowerBlueprintAccess` função com as permissões e relações de confiança adequadas.

A AWSControlTowerBlueprintAccessfunção deve ser configurada para conceder confiança a dois diretores:

- O principal (usuário) que executa o AWS Control Tower na conta de gerenciamento do AWS Control Tower.
- A função nomeada `AWSControlTowerAdmin` na conta de gerenciamento do AWS Control Tower.

Aqui está um exemplo de política de confiança, semelhante à que você precisará incluir para sua função. Essa política demonstra a melhor prática de conceder acesso com privilégios mínimos. Ao criar sua própria política, substitua o termo *`YourManagementAccountId`*pelo ID real da conta de gerenciamento da sua conta de gerenciamento do AWS Control Tower e substitua o

termo *YourControlTowerUserRole*pelo identificador da função do IAM para sua conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Política de permissões necessárias

O AWS Control Tower exige que a política gerenciada nomeada `AWSServiceCatalogAdminFullAccess` seja anexada à `AWSControlTowerBlueprintAccess` função. Essa política fornece permissões que você AWS Service Catalog verifica quando permite que o AWS Control Tower administre seu portfólio e os recursos AWS Service Catalog do produto. Você pode anexar essa política ao criar a função no console do IAM.

Permissões adicionais podem ser necessárias

- Se você armazena seus blueprints no Amazon S3, o AWS Control Tower também exige `AmazonS3ReadOnlyAccess` a política de permissão para `AWSControlTowerBlueprintAccess` a função.
- O tipo de produto AWS Service Catalog Terraform exige que você adicione algumas permissões adicionais à política de IAM personalizada do AFC, caso não utilize a política de administração padrão. Isso é necessário, além das permissões necessárias para criar os recursos que você define em seu modelo de terraform.

## Etapa 2. Crie o AWS Service Catalog produto

Para criar um AWS Service Catalog produto, siga as etapas em Criação de produtos no Guia AWS Service Catalog do administrador. Você adicionará o modelo da sua conta como modelo ao criar o AWS Service Catalog produto.

> **Important**
>
> Como resultado do licenciamento atualizado HashiCorp do Terraform, AWS Service Catalog alterei o suporte aos produtos Terraform Open Source e provisionei os produtos para um novo tipo de produto, chamado Externo. Para saber mais sobre como essa alteração afeta o AFC, incluindo como atualizar seus esquemas de conta existentes para o tipo de produto externo, consulte Transição para o tipo de produto externo.

Resumo das etapas para criar um plano

- Crie ou baixe um AWS CloudFormation modelo ou arquivo de configuração tar.gz do Terraform que se tornará o modelo da sua conta. Alguns exemplos de modelos são fornecidos posteriormente nesta seção.
- Faça login no Conta da AWS local em que você armazena seus blueprints do Account Factory (às vezes chamados de conta central).
- Navegue até o AWS Service Catalog console. Escolha Lista de produtos e, em seguida, escolha Carregar novo produto.
- No painel Detalhes do produto, insira os detalhes do seu produto blueprint, como nome e descrição.
- Selecione Usar um arquivo de modelo e, em seguida, selecione Escolher arquivo. Selecione ou cole o modelo ou arquivo de configuração que você desenvolveu ou baixou para usar como seu blueprint.
- Escolha Criar produto na parte inferior da página do console.

Você pode baixar um AWS CloudFormation modelo do repositório de arquitetura de AWS Service Catalog referência. Um exemplo desse repositório ajuda a configurar um plano de backup para seus recursos.

Aqui está um exemplo de modelo para uma empresa fictícia chamada Best Pets. Isso ajuda a configurar uma conexão com o banco de dados de animais de estimação.

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
 ['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
 " + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn
```

```
  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

### Etapa 3. Revise seu plano personalizado

Você pode ver seu blueprint no AWS Service Catalog console. Para obter mais informações, consulte Gerenciando produtos no Service Catalog Adminstrator Guide.

### Etapa 4. Ligue para seu blueprint para criar uma conta personalizada

Ao seguir o fluxo de trabalho Criar conta no console do AWS Control Tower, você verá uma seção opcional na qual poderá inserir informações sobre o plano que gostaria de usar para personalizar contas.

> **Note**
>
> Você deve configurar sua conta do hub de personalização e adicionar pelo menos um blueprint (produto Service Catalog) antes de poder inserir essas informações no console do AWS Control Tower e começar a provisionar contas personalizadas.

Crie ou atualize uma conta personalizada no console do AWS Control Tower.

1. Insira o ID da conta que contém seus blueprints.
2. Nessa conta, selecione um produto existente do Service Catalog (blueprint existente).
3. Selecione a versão adequada do blueprint (produto Service Catalog), se você tiver mais de uma versão.
4. (Opcional) Você pode adicionar ou alterar uma política de provisionamento de blueprint nesse momento do processo. A política de provisionamento do blueprint é escrita em JSON e anexada a uma função do IAM, para que possa provisionar os recursos especificados no modelo do blueprint. O AWS Control Tower cria essa função na conta do membro para que o Service

Catalog possa implantar recursos usando conjuntos de AWS CloudFormation pilhas. A função é chamada `AWSControlTower-BlueprintExecution-bp-xxxx`. A `AdministratorAccess` política é aplicada aqui por padrão.

5. Escolha as regiões Região da AWS ou regiões nas quais você deseja implantar contas com base nesse blueprint.
6. Se o seu blueprint contiver parâmetros, você poderá inserir os valores dos parâmetros em campos adicionais no fluxo de trabalho do AWS Control Tower. Os valores adicionais podem incluir: um nome de GitHub repositório, uma GitHub filial, um nome de cluster do Amazon ECS e uma GitHub identidade para o proprietário do repositório.
7. Você pode personalizar as contas posteriormente seguindo o processo de atualização da conta, se sua conta central ou seus planos ainda não estiverem prontos.

Para obter mais detalhes, consulte Crie uma conta personalizada a partir de um plano.

## Crie uma conta personalizada a partir de um plano

Depois de criar esquemas personalizados, você pode começar a criar contas personalizadas na fábrica de contas do AWS Control Tower.

Siga estas etapas para implantar um plano personalizado ao criar uma nova AWS conta:

1. Acesse o AWS Control Tower no AWS Management Console.
2. Selecione Fábrica de contas e Criar conta.
3. Insira os detalhes da conta, como nome da conta e endereço de e-mail.
4. Configure os detalhes do IAM Identity Center com endereço de e-mail e nome de usuário.
5. Selecione uma OU registrada na qual sua conta será adicionada.
6. Expanda a seção Personalização de fábrica da conta.
7. Insira o ID da conta do blueprint hub que contém seus produtos do Service Catalog e escolha Validar. Para obter mais informações sobre uma conta do blueprint hub, consultePersonalize contas com Account Factory Customization (AFC).
8. Selecione o menu suspenso que contém todos os blueprints da sua lista de produtos do Service Catalog (todos os blueprints personalizados e de parceiros). Escolha um blueprint e a versão correspondente para implantar.
9. Se o seu blueprint contiver parâmetros, esses campos serão exibidos para você preencher. Os valores padrão são pré-preenchidos.

10. Por fim, selecione onde você implantará seu plano, seja Região de origem ou Todas as regiões governadas. Recursos globais, como Route 53 ou IAM, talvez precisem ser implantados somente em uma única região. Recursos regionais, como instâncias do Amazon EC2 ou buckets do Amazon S3, podem ser implantados em todas as regiões governadas
11. Depois que todos os campos estiverem preenchidos, selecione Criar conta.

> **Note**
>
> Os blueprints criados com o Terraform podem ser implantados somente em uma região, não em várias regiões.

Você pode ver o progresso do provisionamento da sua conta na página Organização. Quando o provisionamento da sua conta estiver concluído, os recursos especificados pelo seu blueprint já estarão implantados nela. Para ver os detalhes da conta e do blueprint, acesse a página Detalhes da conta.

## Inscreva e personalize contas

Para cadastrar e personalizar contas no console do AWS Control Tower.

1. Navegue até o console do AWS Control Tower e selecione Organização no painel de navegação à esquerda.
2. Você verá uma lista das suas contas disponíveis. Identifique a conta que você gostaria de inscrever com um plano personalizado. A coluna Estado dessa conta deve refletir a conta com o status Não inscrito.
3. Selecione o botão de rádio à esquerda da conta e escolha o menu suspenso Ações, no canto superior direito da tela. Aqui você selecionará a opção Inscrever-se.
4. Conclua a seção Configuração de acesso com as informações do IAM Identity Center da conta.
5. Selecione a OU registrada na qual sua conta se tornará membro.
6. Conclua a seção Personalização de fábrica da conta usando as mesmas etapas de 7 a 12 do procedimento Criar conta. Para obter mais informações, consulte Provision Account Factory accounts with AWS Service Catalog.

Você pode ver o status do progresso da sua conta na página Organização. Quando a inscrição da sua conta estiver concluída, os recursos especificados pelo blueprint já estarão implantados nela.

## Adicione um blueprint a uma conta do AWS Control Tower

Para adicionar um blueprint a uma conta de membro existente do AWS Control Tower, siga o fluxo de trabalho de atualização da conta no console do AWS Control Tower e escolha um novo blueprint para adicionar à conta. Para obter mais informações, consulte Atualizar e mover contas do Account Factory com o AWS Control Tower ou com AWS Service Catalog.

> **Note**
>
> Se você adicionar um novo blueprint a uma conta, o blueprint existente será substituído.

> **Note**
>
> Um plano pode ser implantado por conta do AWS Control Tower.

## Atualizar um blueprint

Os procedimentos a seguir descrevem como atualizar os blueprints personalizados e como implantá-los.

Para atualizar seus esquemas personalizados

1. Atualize seu AWS CloudFormation modelo ou arquivo tar.gz (blueprint) do Terraform com suas novas configurações.
2. Salve o blueprint atualizado como uma nova versão em AWS Service Catalog.

Para implantar seu blueprint atualizado

1. Navegue até a página Organização no console do AWS Control Tower.
2. Filtre a página da organização por nome e versão do blueprint.
3. Siga o processo de atualização da conta e implante a versão mais recente do blueprint em sua conta.

Se a atualização do blueprint não for bem-sucedida

O AWS Control Tower permite atualizações do blueprint quando o produto provisionado está no estado. `AVAILABLE` Se o produto provisionado estiver em um `TAINTED` estado, a atualização falhará. Recomendamos a seguinte solução alternativa:

1. No AWS Service Catalog console, atualize manualmente o produto `TAINTED` provisionado para alterar o estado para. `AVAILABLE` Para obter mais informações, consulte Atualização de produtos provisionados.
2. Em seguida, siga o processo de atualização da conta no AWS Control Tower para corrigir o erro de implantação do blueprint.

Recomendamos essa etapa manual porque: Quando você remove um blueprint, isso pode fazer com que os recursos na conta do membro sejam removidos. A remoção de recursos pode afetar suas cargas de trabalho existentes. Por esse motivo, recomendamos esse método em vez da forma alternativa de atualizar um blueprint, que consiste em remover e substituir o blueprint original, especialmente se você estiver executando cargas de trabalho de produção.

## Remover um blueprint de uma conta

Para remover um blueprint de uma conta, siga o fluxo de trabalho Atualizar conta para remover o blueprint e retornar a conta às configurações padrão do AWS Control Tower.

Ao entrar no fluxo de trabalho Atualizar conta no console, você verá que todos os detalhes da conta são preenchidos e os detalhes de personalização não são preenchidos. Se você deixar esses detalhes do AFC em branco, o AWS Control Tower removerá o blueprint da conta. Você verá uma mensagem de aviso antes do início da ação.

> **Note**
>
> O AWS Control Tower adiciona um blueprint a uma conta somente se você selecionar um blueprint durante o processo Criar conta ou Atualizar conta.

## Planos de parceiros

O AWS Control Tower Account Factory Customization (AFC) fornece acesso a esquemas de personalização predefinidos que são criados e gerenciados por parceiros. AWS Esses planos de parceiros ajudam você a personalizar suas contas para casos de uso específicos. Os planos de cada

parceiro ajudam você a criar contas personalizadas, que são pré-configuradas para funcionar com as ofertas de produtos desse parceiro específico.

Para ver uma lista completa dos planos de parceiros do AWS Control Tower, navegue até a Biblioteca de Getting Started do Service Catalog em seu console. Pesquise o tipo de fonte AWS Control Tower Blueprints.

## Considerações sobre Account Factory Customizations (AFC)

- O AFC oferece suporte à personalização usando apenas um único produto de AWS Service Catalog modelo.
- Os produtos do AWS Service Catalog blueprint devem ser criados na conta do hub e na mesma região da região de origem da zona de pouso do AWS Control Tower.
- A função `AWSControlTowerBlueprintAccess` do IAM deve ser criada com o nome, as permissões e a política de confiança adequados.
- O AWS Control Tower oferece suporte a duas opções de implantação para blueprints: implantar somente na região de origem ou implantar em todas as regiões governadas pela AWS Control Tower. A seleção de regiões não está disponível.
- Quando você atualiza um blueprint em uma conta de membro, a ID da conta do blueprint hub e o produto AWS Service Catalog blueprint não podem ser alterados.
- O AWS Control Tower não suporta a remoção de um plano existente e a adição de um novo plano em uma única operação de atualização do plano. Você pode remover um blueprint e depois adicionar um novo blueprint em operações separadas.
- O AWS Control Tower muda o comportamento com base no fato de você estar criando ou inscrevendo contas personalizadas ou contas não personalizadas. Se você não estiver criando ou inscrevendo contas personalizadas com blueprints, o AWS Control Tower cria um produto provisionado pelo Account Factory (por meio do Service Catalog) na conta de gerenciamento da AWS Control Tower. Se você estiver especificando a personalização ao criar ou cadastrar contas com blueprints, o AWS Control Tower não cria um produto provisionado pelo Account Factory na conta de gerenciamento da AWS Control Tower.

## No caso de um erro no blueprint

Erro ao aplicar um blueprint

Se ocorrer um erro durante o processo de aplicação de um plano em uma conta — seja uma conta nova ou uma conta existente que você esteja inscrevendo no AWS Control Tower — o procedimento de recuperação será o mesmo. A conta existirá, mas não é personalizada e não está inscrita no AWS Control Tower. Para continuar, siga as etapas para inscrever a conta no AWS Control Tower e adicionar o plano no momento da inscrição.

Erro ao criar a **`AWSControlTowerBlueprintAccess`** função e soluções alternativas

Ao criar a `AWSControlTowerBlueprintAccess` função a partir de uma conta do AWS Control Tower, você deve estar conectado como principal usando a `AWSControlTowerExecution` função. Se você estiver conectado como qualquer outro, a `CreateRole` operação será impedida por um SCP, conforme mostrado no artefato a seguir:

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
```

```
        }
```

As seguintes soluções alternativas estão disponíveis:

- (Mais recomendado) Assuma a `AWSControlTowerExecution` função e crie a `AWSControlTowerBlueprintAccess` função. Se você escolher essa solução alternativa, certifique-se de sair da `AWSControlTowerExecution` função imediatamente depois, para evitar alterações não intencionais nos recursos.
- Faça login em uma conta que não está inscrita no AWS Control Tower e, portanto, não está sujeita a esse SCP.
- Edite temporariamente esse SCP para permitir a operação.
- (Altamente não recomendado) Use sua conta de gerenciamento do AWS Control Tower como sua conta central, para que ela não esteja sujeita ao SCP.

## Personalizando seu documento de política para esquemas do AFC com base em CloudFormation

Quando você habilita um plano por meio da fábrica de contas, o AWS Control Tower orienta AWS CloudFormation a criação de um StackSet em seu nome. AWS CloudFormation requer acesso à sua conta gerenciada para criar AWS CloudFormation pilhas no StackSet. Embora AWS CloudFormation já tenha privilégios de administrador na conta gerenciada por meio da `AWSControlTowerExecution` função, essa função não pode ser assumida por. AWS CloudFormation

Como parte da habilitação de um plano, o AWS Control Tower cria uma função na conta do membro, que AWS CloudFormation pode assumir a conclusão das tarefas StackSet de gerenciamento. A maneira mais simples de habilitar seu blueprint personalizado por meio do Account Factory é usar uma política de permissão para tudo, pois essas políticas são compatíveis com qualquer modelo de blueprint.

No entanto, as melhores práticas sugerem que você deve restringir as permissões AWS CloudFormation na conta de destino. Você pode fornecer uma política personalizada, que o AWS Control Tower aplica à função criada AWS CloudFormation para uso. Por exemplo, se seu blueprint criar um parâmetro SSM chamado something-important, você poderá fornecer a seguinte política:

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
}
```

A `AllowCloudFormationActionsOnStacks` declaração é obrigatória para todas as políticas personalizadas do AFC; AWS CloudFormation usa essa função para criar instâncias de pilha, portanto, requer permissão para realizar AWS CloudFormation ações em pilhas. A `AllowSsmParameterActions` seção é específica para o modelo que está sendo ativado.

Resolver problemas de permissão

Ao habilitar um blueprint com uma política restrita, você pode descobrir que não há permissões suficientes para habilitar o blueprint. Para resolver esses problemas, revise seu documento de política e atualize as preferências do plano da conta do membro para usar a política corrigida. Para verificar se a política é suficiente para habilitar o blueprint, certifique-se de que as AWS CloudFormation permissões sejam concedidas e que você possa criar uma pilha diretamente usando essa função.

## Permissões adicionais necessárias para criar um produto Service Catalog baseado em Terraform

Ao criar um produto AWS Service Catalog externo com um arquivo de configuração do Terraform para o AFC, é AWS Service Catalog necessário adicionar certas permissões à sua política de IAM personalizada do AFC, além das permissões necessárias para criar os recursos definidos no seu

modelo. Se você escolher a política de administração completa padrão, não precisará adicionar essas permissões extras.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre a criação de produtos Terraform usando o tipo de produto externo em AWS Service Catalog, consulte Etapa 5: Criar funções de lançamento no Service Catalog Administrator Guide.

# Provisione contas com o AWS Control Tower Account Factory for Terraform (AFT)

O AWS Control Tower Account Factory for Terraform (AFT) adota um GitOps modelo que automatiza o processo de provisionamento e atualização de contas na AWS Control Tower.

> **Note**
>
> O AFT não afeta o desempenho do fluxo de trabalho no AWS Control Tower. Se você provisionar uma conta por meio do AFT ou do Account Factory, o mesmo fluxo de trabalho de back-end ocorrerá.

Com o AFT, você cria um arquivo Terraform de solicitação de conta, que contém a entrada que invoca o fluxo de trabalho do AFT. Após o término do provisionamento e da atualização da conta, o fluxo de trabalho do AFT continua executando a estrutura de provisionamento de contas do AFT e as etapas de personalização da conta.

## Pré-requisitos

Antes de começar a usar o AFT, você deve criar o seguinte:

- Um ambiente AFT totalmente implantado. Para obter mais informações, consulte Visão geral do AWS Control Tower Account Factory for Terraform (AFT) e Implante o AWS Control Tower Account Factory for Terraform (AFT)
- Um ou mais `git` repositórios AFT em seu ambiente AFT totalmente implantado. Para obter mais informações, consulte Etapas de pós-implantação do AFT.

> **Tip**
>
> Opcionalmente, você pode criar uma pasta de modelo de conta no aft-account-customizationsrepositório.

Para obter informações sobre Regiões da AWS onde o AFT tem limitações de implantação, consulte Limitações e cotas na AWS Control Tower Limitações de controle e.

# Provisionar uma nova conta com a AFT

Para provisionar uma nova conta com o AFT, crie um arquivo Terraform de solicitação de conta. Esse arquivo contém a entrada para parâmetros no aft-account-requestrepositório. Depois de criar um arquivo Terraform de solicitação de conta, comece a processar sua solicitação de conta executando`git push`. Esse comando invoca a `ct-aft-account-request` operação no AWS CodePipeline, que é criada na conta de gerenciamento do AFT após a conclusão do provisionamento da conta. Para obter mais informações, consulte Pipeline de provisionamento de contas AFT.

## Parâmetros do arquivo Terraform de solicitação de conta

Você deve incluir os seguintes parâmetros no arquivo Terraform de solicitação de conta. Você pode ver um exemplo de arquivo Terraform de solicitação de conta em. GitHub

- O valor de `module name` deve ser exclusivo de acordo com a Conta da AWS solicitação.
- O valor de `module source` é o caminho para o módulo Terraform de solicitação de conta que o AFT fornece.
- O valor de `control_tower_parameters` captura a entrada necessária para criar uma conta do AWS Control Tower. O valor inclui os seguintes campos de entrada:
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> A entrada que você fornece não `control_tower_parameters` pode ser alterada durante o provisionamento da conta.
> Os formatos compatíveis para especificação `ManagedOrganizationalUnit` no aft-account-requestrepositório incluem e. `OUName` `OUName (OU-ID)`

- `account_tags`captura chaves e valores definidos pelo usuário, que podem ser marcados de Contas da AWS acordo com os critérios comerciais. Para obter mais informações, consulte Marcar AWS Organizations recursos no Guia do AWS Organizations usuário.
- O valor de `change_management_parameters` captura informações adicionais, como por que uma solicitação de conta foi criada e quem iniciou a solicitação de conta. O valor inclui os seguintes campos de entrada:
  - `change_reason`
  - `change_requested_by`
- `custom_fields`captura metadados adicionais com chaves e valores que são implantados como parâmetros SSM na conta vendida em /aft/account-request/custom-fields/. Você pode consultar esses metadados durante as personalizações da conta para implantar os controles adequados. Por exemplo, uma conta sujeita à conformidade regulatória pode implantar outras Regras do AWS Config. Os metadados que você coleta `custom_fields` podem invocar processamento adicional durante o provisionamento e a atualização da conta. Se um campo personalizado for removido da solicitação de conta, o campo personalizado será removido do SSM Parameter Store da conta vendida.
- (Opcional) `account_customizations_name` captura a pasta do modelo de conta no aft-account-customizationsrepositório. Para obter mais informações, consulte Personalizações da conta.

## Envie várias solicitações de conta

O AFT processa as solicitações de conta uma por vez, mas você pode enviar várias solicitações de conta para o pipeline do AFT. Quando você envia várias solicitações de conta para o pipeline do AFT, o AFT enfileira e processa as solicitações da conta em uma ordem de primeiro a entrar e primeiro a sair.

> **Note**
>
> Você pode criar um arquivo Terraform de solicitação de conta para cada conta que você deseja que o AFT provisione ou distribua várias solicitações de conta em um único arquivo Terraform de solicitação de conta.

## Atualizar uma conta existente

Você pode atualizar as contas provisionadas pelo AFT editando as solicitações de conta enviadas anteriormente e executando`git push`. Esse comando invoca o fluxo de trabalho de provisionamento da conta e pode processar solicitações de atualização da conta. Você pode atualizar a entrada para`ManagedOrganizationalUnit`, que faz parte do valor necessário para`control_tower_parameters`, e outros parâmetros no arquivo Terraform de solicitação de conta. Para obter mais informações, consulte Provisionar uma nova conta com a AFT.

> **Note**
>
> A entrada que você fornece não `control_tower_parameters` pode ser alterada durante o provisionamento da conta.
> Os formatos compatíveis para especificação `ManagedOrganizationalUnit` no aft-account-requestrepositório incluem e. `OUName` `OUName (OU-ID)`

### Atualizar uma conta que a AFT não provisiona

Você pode atualizar as contas do AWS Control Tower criadas fora do AFT especificando a conta no aft-account-requestrepositório.

> **Note**
>
> Certifique-se de que todos os detalhes da conta estejam corretos e consistentes com a organização do AWS Control Tower e o respectivo produto AWS Service Catalog provisionado.

Pré-requisitos para atualizar um existente com o AFT Conta da AWS

- Eles Conta da AWS devem estar inscritos no AWS Control Tower.
- Eles Conta da AWS devem fazer parte da organização do AWS Control Tower.

## Implante AWS o Control Tower Account Factory para Terraform () AFT

Esta seção é para administradores de ambientes AWS Control Tower que desejam configurar o Account Factory for Terraform (AFT) em seu ambiente existente. Ele descreve como configurar

um ambiente Account Factory for Terraform (AFT) com uma nova conta AFT de gerenciamento dedicada.

> **Note**
>
> Um módulo Terraform é AFT implantado. Esse módulo está disponível no AFTrepositório em GitHub, e todo o AFT repositório é considerado o módulo.
> Recomendamos que você consulte os AFT módulos em GitHub vez de clonar o AFT repositório. Dessa forma, você pode controlar e consumir atualizações dos módulos à medida que estiverem disponíveis.

Para obter detalhes sobre as versões mais recentes da funcionalidade AWS Control Tower Account Factory for Terraform (AFT), consulte o arquivo de lançamentos desse GitHub repositório.

Pré-requisitos de implantação

Antes de configurar e iniciar seu AFT ambiente, você deve ter o seguinte:

- Uma zona de pouso da AWS Control Tower. Para obter mais informações, consulte Planejar sua zona de pouso da AWS Control Tower.
- Uma região de origem para sua landing zone da AWS Control Tower. Para obter mais informações, consulte Como Regiões da AWS trabalhar com a AWS Control Tower.
- Uma versão e distribuição do Terraform. Para obter mais informações, consulte Terraform e AFT versões.
- Um VCS provedor para rastrear e gerenciar alterações no código e em outros arquivos. Por padrão, AFT usa AWS CodeCommit. Para obter mais informações, consulte O que é AWS CodeCommit? no Guia do AWS CodeCommit usuário.

  Se você estiver implantando AFT pela primeira vez e não tiver um CodeCommit repositório existente, deverá escolher um VCS provedor externo, como GitHub ou. BitBucket Para obter mais informações, consulte Alternativas para controle de versão do código-fonte em AFT.
- Um ambiente de execução em que você pode executar o módulo Terraform que é instaladoAFT.
- AFTopções de recursos. Para obter mais informações, consulte Habilitar opções de recursos.

## Configure e inicie sua AWS Control Tower Account Factory para Terraform

As etapas a seguir pressupõem que você esteja familiarizado com o fluxo de trabalho do Terraform. Você também pode aprender mais sobre a implantação AFT seguindo a Introdução ao AFT laboratório no site do AWS Workshop Studio.

Etapa 1: Inicie sua zona de pouso da AWS Control Tower

Conclua as etapas em Introdução ao AWS Control Tower. É aqui que você cria a conta de gerenciamento da AWS Control Tower e configura sua zona de pouso da AWS Control Tower.

> **Note**
>
> Certifique-se de criar uma função para a conta de gerenciamento da AWS Control Tower que tenha AdministratorAccesscredenciais. Para obter mais informações, consulte as informações a seguir.
>
> - IAMIdentidades (usuários, grupos de usuários e funções) no Guia do AWS Identity and Access Management usuário
> - AdministratorAccessno Guia de referência de políticas AWS gerenciadas

Etapa 2: criar uma nova unidade organizacional para AFT (recomendado)

Recomendamos que você crie uma OU separada em sua AWS organização. É aqui que você implanta a conta AFT de gerenciamento. Crie a nova OU com sua conta de gerenciamento da AWS Control Tower. Para obter mais informações, consulte Criar uma nova OU.

Etapa 3: provisionar a conta AFT de gerenciamento

AFTexige que você provisione uma AWS conta dedicada às operações AFT de gerenciamento. A conta de gerenciamento da AWS Control Tower, associada à sua landing zone da AWS Control Tower, vende a conta AFT de gerenciamento. Para obter mais informações, consulte Provisionar contas com o AWS Service Catalog Account Factory.

> **Note**
>
> Se você criou uma OU separada paraAFT, certifique-se de selecionar essa OU ao criar a conta AFT de gerenciamento.

Pode levar até 30 minutos para provisionar totalmente a conta AFT de gerenciamento.

Etapa 4: Verificar se o ambiente Terraform está disponível para implantação

Esta etapa pressupõe que você tenha experiência com o Terraform e tenha procedimentos implementados para executar o Terraform. Para obter mais informações, consulte Command: init no site do HashiCorp desenvolvedor.

> **Note**
>
> AFTsuporta a versão Terraform `1.6.0` ou posterior.

Etapa 5: chame o módulo Account Factory for Terraform para implantar AFT

Chame o AFT módulo com a função que você criou para a conta de gerenciamento da AWS Control Tower que tem AdministratorAccesscredenciais. AWSO Control Tower provisiona um módulo Terraform por meio da conta de gerenciamento da AWS Control Tower, que estabelece toda a infraestrutura necessária para orquestrar as solicitações do Control AWS Tower Account Factory.

Você pode visualizar o AFT módulo no AFTrepositório em. GitHub O GitHub repositório inteiro é considerado o AFT módulo. Consulte o READMEarquivo para obter informações sobre as entradas necessárias para executar o AFT módulo e implantarAFT. Como alternativa, você pode visualizar o AFT módulo no Registro do Terraform.

O AFT módulo inclui um `aft_enable_vpc` parâmetro que especifica se o AWS Control Tower provisiona recursos da conta em uma nuvem privada virtual (VPC) na conta AFT de gerenciamento central. Por padrão, o parâmetro é definido como`true`. Se você definir esse parâmetro como`false`, o AWS Control Tower será implantado AFT sem o uso de VPC recursos de rede privados, como NAT gateways ou VPC endpoints. A desativação `aft_enable_vpc` pode ajudar a reduzir o custo operacional AFT de alguns padrões de uso.

> **Note**
>
> A reativação do `aft_enable_vpc` parâmetro (alternando o valor de `false` para`true`) pode exigir que você execute o `terraform apply` comando duas vezes consecutivas.

Se você tiver pipelines em seu ambiente que estão estabelecidos para gerenciar o Terraform, você pode integrar o AFT módulo ao seu fluxo de trabalho existente. Caso contrário, execute o AFT módulo em qualquer ambiente autenticado com as credenciais necessárias.

O tempo limite faz com que a implantação falhe. Recomendamos usar as credenciais AWS Security Token Service (STS) para garantir que você tenha um tempo limite suficiente para uma implantação completa. O tempo limite mínimo para AWS STS credenciais é de 60 minutos. Para obter mais informações, consulte Credenciais de segurança temporárias IAM no Guia do AWS Identity and Access Management usuário.

> **Note**
>
> Você pode esperar até 30 minutos para concluir AFT a implantação por meio do módulo Terraform.

Etapa 6: gerenciar o arquivo de estado do Terraform

Um arquivo de estado do Terraform é gerado quando você implantaAFT. Esse artefato descreve o estado dos recursos que o Terraform criou. Se você planeja atualizar a AFT versão, certifique-se de preservar o arquivo de estado do Terraform ou configurar um back-end do Terraform usando o Amazon S3 e o DynamoDB. O AFT módulo não gerencia um estado de back-end do Terraform.

> **Note**
>
> Você é responsável por proteger o arquivo de estado do Terraform. Algumas variáveis de entrada podem conter valores confidenciais, como uma `ssh` chave privada ou um token do Terraform. Dependendo do seu método de implantação, esses valores podem ser visualizados como texto simples no arquivo de estado do Terraform. Para obter mais informações, consulte Dados confidenciais no estado no HashiCorp site.

## Etapas de pós-implantação

Depois que a implantação da AFT infraestrutura for concluída, siga estas etapas adicionais para concluir o processo de configuração e se preparar para provisionar contas.

Etapa 1: complete CodeConnections com o VCS provedor desejado

Se você escolher um VCS provedor terceirizado CodeConnections, AFT estabelece e confirma. Consulte Alternativas para controle de versão do código-fonte em AFT para saber como configurar AFT com sua preferênciaVCS.

A etapa inicial de estabelecer a AWS CodeStar conexão é realizada porAFT. Você deve confirmar a conexão.

Etapa 2: preencher cada repositório

AFTexige que você gerencie quatro repositórios:

1. Solicitações de conta — Esse repositório lida com a colocação ou atualização de solicitações de conta. Exemplos disponíveis. Para obter mais informações sobre solicitações de AFT conta, consulteProvisionar uma nova conta com a AFT.
2. AFTpersonalizações de provisionamento de contas — Esse repositório gerencia personalizações que são aplicadas a todas as contas criadas e gerenciadas comAFT, antes de iniciar o estágio global de personalizações. Exemplos disponíveis. Para criar personalizações de provisionamento de AFT contas, consulte. Crie sua conta AFT, provisionando, personalizações, máquina de estado
3. Personalizações globais — Esse repositório gerencia personalizações que são aplicadas a todas as contas criadas e gerenciadas com. AFT Exemplos disponíveis. Para criar personalizações AFT globais, consulte. Aplique personalizações globais
4. Personalizações de conta — Esse repositório gerencia personalizações que são aplicadas somente a contas específicas criadas e gerenciadas com. AFT Exemplos disponíveis. Para criar personalizações de AFT conta, consulte. Aplique personalizações de conta

AFTespera que cada um desses repositórios siga uma estrutura de diretórios específica. Os modelos usados para preencher seus repositórios e as instruções que descrevem como preencher os modelos estão disponíveis no módulo Account Factory for Terraform no repositório github. AFT

## Visão geral do AWS Control Tower Account Factory for Terraform () AFT

O Account Factory for Terraform (AFT) configura um pipeline do Terraform para ajudá-lo a provisionar e personalizar contas na AWS Control Tower. AFToferece a vantagem do provisionamento de contas baseado no Terraform, ao mesmo tempo em que permite que você controle suas contas com a Control Tower. AWS

Com AFT você, crie um arquivo Terraform de solicitação de conta para obter a entrada que aciona o AFT fluxo de trabalho para o provisionamento da conta. Depois que o estágio de provisionamento da

conta for concluído, AFT executará automaticamente uma série de etapas antes do início do estágio de personalização da conta. Para obter mais informações, consulte Pipeline de provisionamento de AFT contas.

AFTé compatível com Terraform Cloud, Terraform Enterprise e Terraform Community Edition. Com AFT você pode iniciar a criação da conta usando um arquivo de entrada e um `git push` comando simples e personalizar contas novas ou existentes. A criação de contas inclui todos os benefícios de governança e personalizações de contas da AWS Control Tower que ajudam você a cumprir os procedimentos de segurança padrão e as diretrizes de conformidade da sua organização.

AFToferece suporte ao rastreamento de solicitações de personalização da conta. Toda vez que você envia uma solicitação de personalização de conta, AFT gera um token de rastreamento exclusivo que passa por uma máquina de AWS Step Functions estado de AFT personalização, que registra o token como parte de sua execução. Em seguida, você pode usar as consultas de insights do Amazon CloudWatch Logs para pesquisar intervalos de timestamp e recuperar o token da solicitação. Como resultado, você pode ver as cargas que acompanham o token, para que você possa rastrear sua solicitação de personalização da conta em todo AFT o fluxo de trabalho. Para obter informações sobre CloudWatch Logs e Step Functions, consulte o seguinte:

- O que é o Amazon CloudWatch Logs? no Guia do usuário do Amazon CloudWatch Logs
- O que AWS Step Functionsé no Guia do AWS Step Functions desenvolvedor

AFTcombina os recursos de outros AWS serviçosServiços de componentes, como criar uma estrutura, com pipelines que implantam o Terraform Infrastructure as Code (IaC). O AFT permite:

- Envie solicitações de provisionamento e atualização de contas em um modelo GitOps
- Armazene metadados da conta e histórico de auditoria
- Aplique tags no nível da conta
- Adicione personalizações a todas as contas, a um conjunto de contas ou a contas individuais
- Ativar opções de recursos

AFTcria uma conta separada, chamada de conta AFT de gerenciamento, para implantar AFT recursos. Antes de fazer a configuraçãoAFT, você deve ter uma landing zone existente da AWS Control Tower. A conta AFT de gerenciamento não é a mesma que a conta de gerenciamento da AWS Control Tower.

AFToferece flexibilidade

- Flexibilidade para sua plataforma: AFT suporta qualquer distribuição do Terraform para implantação inicial e operação contínua: Community Edition, Cloud e Enterprise.
- Flexibilidade para seu sistema de controle de versão: AFT suportes AWS CodeCommit e fontes alternativas de controle de versão por meio de Conexões de código da AWS.

### AFToferece opções de recursos

Você pode ativar várias opções de recursos, com base nas melhores práticas:

- Criação de um nível organizacional CloudTrail para registrar eventos de dados
- Excluindo o AWS padrão VPC para contas
- Inscrevendo contas provisionadas no plano Enterprise Support AWS

> **Note**
>
> O AFT pipeline não se destina ao uso na implantação de recursos, como EC2 instâncias da Amazon, que suas contas precisam para executar seus aplicativos. Ele se destina exclusivamente ao provisionamento e personalização automatizados de contas da AWS Control Tower.

## Passo a passo em vídeo

Este vídeo (7:33) descreve como implantar contas com o AWS Control Tower Account Factory for Terraform. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Passo a passo em vídeo do provisionamento automatizado de contas na Control Tower. AWS

## AFTArquitetura

### Ordem das operações

Você executa AFT operações na conta AFT de gerenciamento. Para um fluxo de trabalho completo de provisionamento de contas, a ordem dos estágios da esquerda para a direita no diagrama é a seguinte:

1. As solicitações de conta são criadas e enviadas ao pipeline. Você pode criar e enviar mais de uma solicitação de conta por vez. O Account Factory processa solicitações em um first-in-first-out pedido. Para obter mais informações, consulte Enviar várias solicitações de conta.
2. Cada conta é provisionada. Esse estágio é executado na conta de gerenciamento da AWS Control Tower.
3. As personalizações globais são executadas nos pipelines criados para cada conta vendida.
4. Se as personalizações forem especificadas nas solicitações iniciais de provisionamento da conta, as personalizações serão executadas somente nas contas específicas. Se você tem uma conta que já está provisionada, você deve iniciar outras personalizações manualmente no funil da conta.

AWSControl Tower Account Factory for Terraform — fluxo de trabalho de provisionamento de contas

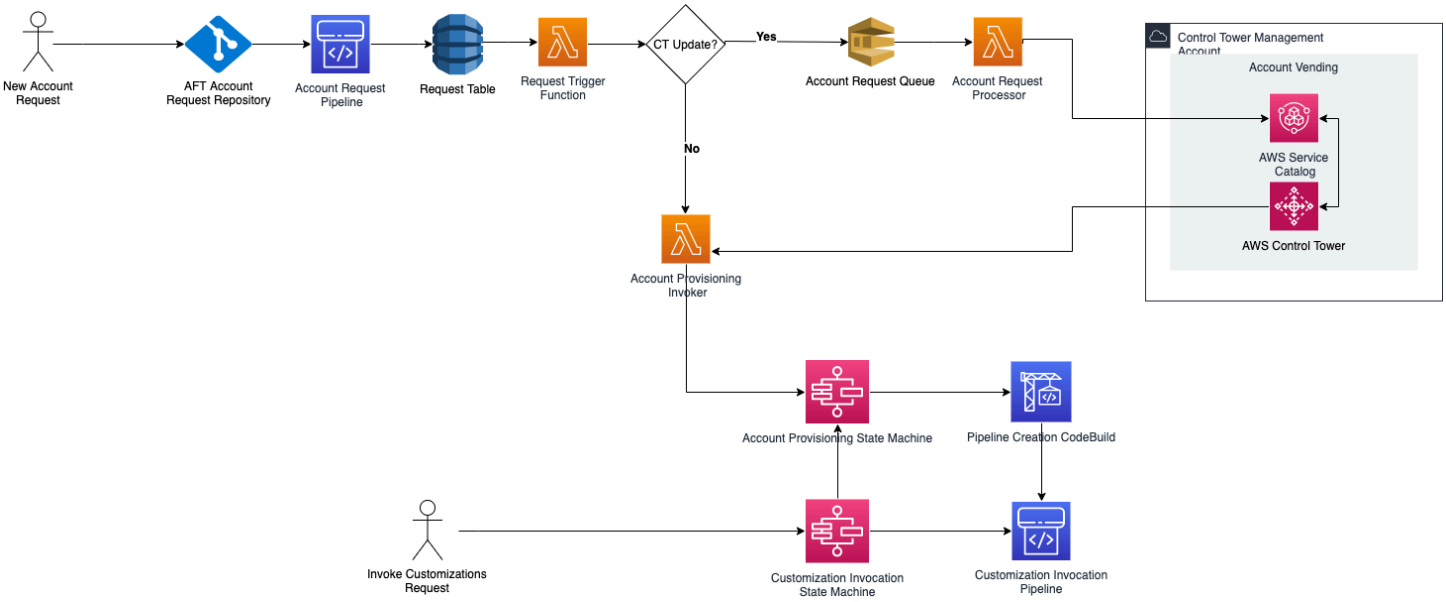


Figura 1: AWS Control Tower Account Factory para Terraform

## Custo

Não existe nenhum custo adicional paraAFT. Você paga somente pelos recursos implantadosAFT, pelos AWS serviços habilitados e pelos AFT recursos implantados em seu AFT ambiente.

A AFT configuração padrão inclui a alocação de AWS PrivateLink endpoints, para maior proteção e segurança de dados, e um NAT gateway que é necessário para oferecer suporte. AWS CodeBuild Para obter detalhes sobre os preços dessa infraestrutura, consulte os AWS PrivateLink preços e os preços da Amazon VPC para o NAT Gateway. Entre em contato com seu representante de AWS

conta para obter informações mais específicas sobre como gerenciar esses custos. Você pode alterar essas configurações padrão paraAFT.

## Versões Terraform e AFT

O Account Factory for Terraform (AFT) suporta a versão Terraform `1.6.0` ou posterior. Você deve fornecer uma versão do Terraform como parâmetro de entrada para o processo de implantação do AFT, conforme mostrado no exemplo a seguir.

```
terraform_version = "1.6.0"
```

### Distribuições do Terraform

O AFT suporta três distribuições do Terraform:

- Edição Comunitária do Terraform
- Nuvem Terraform
- Terraform Enterprise

Essas distribuições são explicadas nas seções a seguir. Forneça a distribuição Terraform de sua escolha como um parâmetro de entrada durante o processo de bootstrap do AFT. Para obter mais informações sobre a implantação do AFT e os parâmetros de entrada, consulteImplante AWS o Control Tower Account Factory para Terraform () AFT.

Se você escolher as distribuições Terraform Cloud ou Terraform Enterprise, o token de API especificado `terraform_token` deverá ser um token de API de usuário ou equipe. Um token de organização não é compatível com todas as APIs necessárias. Por motivos de segurança, você deve evitar verificar o valor desse token em seu sistema de controle de versão (VCS) atribuindo uma variável de terraform, conforme mostrado no exemplo a seguir.

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

#### Edição Comunitária do Terraform

Quando você seleciona o Terraform Community Edition como sua distribuição, o AFT gerencia o back-end do Terraform para você na conta de gerenciamento do AFT. O AFT baixa a versão

especificada `terraform-cli` do Terraform para ser executada durante a implantação do AFT e as fases do pipeline do AFT. A configuração de estado resultante do Terraform é armazenada em um bucket Amazon S3, nomeado com o seguinte formato:

```
aft-backend-[account_id]-primary-region
```

O AFT também cria um bucket Amazon S3 que replica sua configuração de estado do Terraform em outro Região da AWS, para fins de recuperação de desastres, nomeado com o seguinte formato:

```
aft-backend-[account_id]-secondary-region
```

Recomendamos que você habilite a autenticação multifator (MFA) para funções de exclusão nesses buckets Amazon S3 do estado do Terraform. Para saber mais sobre o Terraform Community Edition, consulte a documentação do Terraform.

Para selecionar o Terraform OSS como sua distribuição, forneça o seguinte parâmetro de entrada:

```
terraform_distribution = "oss"
```

Nuvem Terraform

Quando você seleciona o Terraform Cloud como sua distribuição, o AFT cria espaços de trabalho para os seguintes componentes em sua organização do Terraform Cloud, o que inicia um fluxo de trabalho orientado por API.

- Solicitação de conta
- Personalizações do AFT para contas provisionadas pelo AFT
- Personalizações de conta para contas provisionadas pela AFT
- Personalizações globais para contas provisionadas pela AFT

O Terraform Cloud gerencia a configuração de estado resultante do Terraform.

Ao selecionar o Terraform Cloud como sua distribuição, forneça os seguintes parâmetros de entrada:

- `terraform_distribution = "tfc"`
- `terraform_token`— Esse parâmetro contém o valor do token do Terraform Cloud. O AFT marca o como confidencial e armazena o valor como uma string segura no armazenamento

de parâmetros SSM na conta de gerenciamento do AFT. Recomendamos que você alterne periodicamente o valor do token Terraform de acordo com as políticas de segurança e as diretrizes de conformidade da sua empresa. O token do Terraform deve ser um token de API de nível de usuário ou equipe. Os tokens da organização não são suportados.

- `terraform_org_name`— Esse parâmetro contém o nome da sua organização do Terraform Cloud.

> **Note**
>
> Não há suporte para várias implantações de AFT em uma única organização do Terraform Cloud.

Para obter informações sobre como configurar o Terraform Cloud, consulte a documentação do Terraform.

Terraform Enterprise

Quando você seleciona o Terraform Enterprise como sua distribuição, o AFT cria espaços de trabalho para os seguintes componentes em sua organização do Terraform Enterprise e aciona um fluxo de trabalho orientado por API para as execuções resultantes do Terraform.

- Solicitação de conta
- Personalizações de provisionamento de contas AFT para contas provisionadas pela AFT
- Personalizações de conta para contas provisionadas pela AFT
- Personalizações globais para contas provisionadas pela AFT

A configuração de estado resultante do Terraform é gerenciada pela configuração do Terraform Enterprise.

Para selecionar o Terraform Enterprise como sua distribuição, forneça os seguintes parâmetros de entrada:

- `terraform_distribution = "tfe"`
- `terraform_token`— Esse parâmetro contém o valor do seu token do Terraform Enterprise. O AFT marca seu valor como confidencial e o armazena como uma string segura no armazenamento

de parâmetros SSM, na conta de gerenciamento do AFT. Recomendamos que você alterne periodicamente o valor do token Terraform, de acordo com as políticas de segurança e as diretrizes de conformidade da sua empresa.

- `terraform_org_name`— Esse parâmetro contém o nome da sua organização Terraform Enterprise.
- `terraform_api_endpoint`— Esse parâmetro contém a URL do seu ambiente Terraform Enterprise. O valor desse parâmetro deve estar no formato:

```
https://{fqdn}/api/v2/
```

Consulte a documentação do Terraform para saber mais sobre como configurar o Terraform Enterprise.

## Verifique a versão AFT

Você pode verificar sua versão do AFT implantada consultando a chave AWS SSM Parameter Store:

```
/aft/config/aft/version
```

Se você usar o método de registro, poderá fixar a versão.

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

Você pode ver mais informações sobre as versões do AFT no repositório do AFT.

## Atualize a versão AFT

Você pode atualizar sua versão implantada do AFT retirando-a da ramificação do `main` repositório:

```
terraform get -update
```

Depois que a extração for concluída, você poderá executar novamente o plano do Terraform ou executar a aplicação para atualizar a infraestrutura do AFT com as alterações mais recentes.

# Ativar opções de recursos

O AFT oferece opções de recursos com base nas melhores práticas. Você pode optar por esses recursos, por meio de sinalizadores de recursos, durante a implantação do AFT. Consulte Provisionar uma nova conta com a AFT para obter mais informações sobre os parâmetros de configuração de entrada AFT.

Esses recursos não estão habilitados por padrão. Você deve habilitar explicitamente cada um em seu ambiente.

Tópicos

- AWS CloudTrail eventos de dados
- AWS Plano de Enterprise Support
- Exclua a AWS VPC padrão

## AWS CloudTrail eventos de dados

Quando ativada, a opção AWS CloudTrail de eventos de dados configura esses recursos.

- Cria uma trilha organizacional na conta de gerenciamento do AWS Control Tower, para CloudTrail
- Ativa o registro em log para eventos de dados do Amazon S3 e do Lambda
- Criptografa e exporta todos os eventos de CloudTrail dados para um bucket `aws-aft-logs-*` S3 na conta do AWS Control Tower Log Archive, com criptografia AWS KMS
- Ativa a configuração de validação do arquivo de log

Para habilitar essa opção, defina o seguinte sinalizador de recurso como True em sua configuração de entrada de implantação do AFT.

```
aft_feature_cloudtrail_data_events
```

Pré-requisito

Antes de habilitar essa opção de recurso, certifique-se de que o acesso confiável para AWS CloudTrail esteja habilitado em sua organização.

Para verificar o status do acesso confiável para CloudTrail :

1. Navegue até o AWS Organizations console.

2. Escolha Serviços > CloudTrail.
3. Em seguida, selecione Habilitar acesso confiável no canto superior direito, se necessário.

Você pode receber uma mensagem de aviso recomendando o uso do AWS CloudTrail console, mas, nesse caso, ignore o aviso. O AFT cria a trilha como parte da ativação dessa opção de recurso, depois que você permite o acesso confiável. Se o acesso confiável não estiver habilitado, você receberá uma mensagem de erro quando o AFT tentar criar sua trilha para eventos de dados.

> **Note**
>
> Essa configuração funciona no nível da organização. A ativação dessa configuração afeta todas as contas AWS Organizations, sejam elas gerenciadas pelo AFT ou não. Todos os buckets na conta do AWS Control Tower Log Archive no momento da ativação estão excluídos dos eventos de dados do Amazon S3. Consulte o Guia AWS CloudTrail do usuário para saber mais sobre CloudTrail.

## AWS Plano de Enterprise Support

Quando essa opção está ativada, o pipeline AFT ativa o plano AWS Enterprise Support para contas provisionadas pela AFT.

AWS Por padrão, as contas vêm com o plano AWS Basic Support ativado. O AFT fornece inscrição automática no nível de suporte corporativo para contas provisionadas pelo AFT. O processo de provisionamento abre um ticket de suporte para a conta, solicitando que ela seja adicionada ao plano Enterprise AWS Support.

Para habilitar a opção Enterprise Support, defina o seguinte sinalizador de recurso como True em sua configuração de entrada de implantação do AFT.

```
aft_feature_enterprise_support=false
```

Consulte Compare AWS Support Plans para saber mais sobre AWS Support Plans.

> **Note**
>
> Para permitir que esse recurso funcione, você deve inscrever a conta pagante no plano Enterprise Support.

### Exclua a AWS VPC padrão

Quando você ativa essa opção, o AFT exclui todas as VPCs AWS padrão na conta de gerenciamento e em todas Regiões da AWS, mesmo que não tenha implantado recursos do AWS Control Tower nelas. Regiões da AWS

O AFT não exclui automaticamente as VPCs AWS padrão de nenhuma conta da AWS Control Tower provisionada pelo AFT ou de AWS contas existentes que você inscreva na AWS Control Tower por meio do AFT.

Novas AWS contas são criadas com uma VPC configurada em cada uma Região da AWS, por padrão. Sua empresa pode ter práticas padrão para criar VPCs, que exigem que você exclua a VPC AWS padrão e evite ativá-la, especialmente para a conta de gerenciamento do AFT.

Para habilitar essa opção, defina o seguinte sinalizador de recurso como True em sua configuração de entrada de implantação do AFT.

```
aft_feature_delete_default_vpcs_enabled
```

Consulte VPC padrão e sub-redes padrão para saber mais sobre VPCs padrão.

## Considerações sobre recursos para o AWS Control Tower Account Factory for Terraform

Quando você configura sua landing zone usando o AWS Control Tower Account Factory for Terraform, vários tipos de AWS recursos são criados em suas AWS contas.

Pesquise recursos

- Você pode usar tags para pesquisar a lista mais atualizada de recursos do AFT. O par de valores-chave para sua pesquisa é:

  ```
  Key: managed_by | Value: AFT
  ```

- Para serviços de componentes que não oferecem suporte a tags, você pode localizar recursos com uma pesquisa `aft` nos nomes dos recursos.

Tabelas de recursos inicialmente criadas, por conta

Conta de gerenciamento do AWS Control Tower Account Factory for Terraform

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | AWSAFTAdministrator<br>AWSAFTExecution<br>AWSAFTService<br>aws-ct-aft-* |
| AWS Identity and Access Management | Políticas | aws-ct-aft-* |
| CodeCommit | Repositórios | aws-ct-aft-* |
| CodeBuild | Projetos de build | aws-ct-aft-* |
| Pipeline de código | Pipelines | *-baseline-* |
| Amazon S3 | Buckets | *-aws-ct-aft-*<br>aws-ct-aft-* |
| Lambda | Funções | aws-ct-aft-* |
| Lambda | Camadas | aws-ct-aft-common-layer |
| DynamoDB | Tabelas | aws-ct-aft-request<br>aws-ct-aft-request-audit<br>aws-ct-aft-request-metadata<br>aws-ct-aft-controltower-events |
| Step Functions | Máquinas estatais | aws-ct-aft-prebaseline<br>aws-ct-aft-prebaseline-customizations<br>aws-ct-aft-trigger-baseline |

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| | | aws-ct-aft-features |
| VPC | VPC | aws-ct-aft-vpc |
| Amazon SNS | Tópicos | aws-ct-aft-notifications<br>aws-ct-aft-failure-notifications |
| Amazon EventBridge | Barramentos de eventos | aws-ct-aft-events-from-ct-management |
| Amazon EventBridge | Regras do evento | aws-ct-aft-capture-ct-events<br>aws-ct-aft-lambda-account-request-processor |
| Serviço de gerenciamento de chaves (KMS) | Chaves gerenciadas pelo cliente | *-aws-ct-aft-*<br>aws-ct-aft-* |
| AWS Systems Manager | Armazenamento de parâmetros | /aws-ct-aft/account/*<br>/aws/ct-aft/config/* |
| Amazon SQS | Filas | aws-ct-aft-account-request.fifo<br>aws-ct-aft-account-request-dlg.fifo |
| CloudWatch | Grupos de logs | /aws/*/aws-ct-aft-*<br>aws-ct-aft-* |
| AWS Support Center (opcional) | Planos de suporte | Enterprise |

AWS contas provisionadas por meio do AWS Control Tower Account Factory for Terraform

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | AWSAFTExecution |
| AWS Support Center (opcional) | Planos de suporte | Enterprise |

Conta de gerenciamento do AWS Control Tower

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | AWSAFTExecutionRole<br>AWSAFTExecution<br>aws-ct-aft-controltower-events-rule |
| AWS Systems Manager | Armazenamento de parâmetros | /aws-ct-aft/account/aws-ct-aft-management/account-id |
| AWS Organizations (Opcional) | Políticas de controle de serviço | aws-ct-aft-protect-resources |
| CloudTrail (Opcional) | Trilhas | aws-ct-aft-BaselineCloudTrail |
| Centro de suporte da AWS (opcional) | Planos de suporte | Enterprise |

Conta de arquivo de log do AWS Control Tower

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | AWSAFTExecutionRole<br>AWSAFTExecution |

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| | | aws-ct-aft-cloudtrail-data-events-role |
| Serviço de gerenciamento de chaves (KMS) | Chaves gerenciadas pelo cliente | *-aws-ct-aft-kms-gd-findings |
| Amazon S3 | Buckets | *-aws-ct-aft-logs*<br>aws-ct-aft-s3-access-logs* |
| AWS Support Center (opcional) | Planos de suporte | Enterprise |

Conta de auditoria do AWS Control Tower

| AWS serviço | Tipo de atributo | Nome do recurso |
| --- | --- | --- |
| AWS Identity and Access Management | Funções | AWSAFTExecutionRole<br>AWSAFTExecution |
| AWS Support Center (opcional) | Planos de suporte | Enterprise |

## Funções necessárias

Em geral, funções e políticas fazem parte do gerenciamento de identidade e acesso (IAM) em AWS. Consulte o GuiaAWS do usuário do IAM para obter mais informações.

O AFT cria várias funções e políticas do IAM nas contas de gerenciamento do AFT e do AWS Control Tower para apoiar as operações do pipeline do AFT. Essas funções são criadas com base no modelo de acesso com privilégios mínimos, que restringe a permissão aos conjuntos de ações e recursos minimamente necessários para cada função e política. Essas funções e políticas recebem um `key:value` par de AWS tags, `managed_by:AFT` para identificação.

Além dessas funções do IAM, a AFT cria três funções essenciais:

- o `AWSAFTAdmin` papel
- o `AWSAFTExecution` papel
- o `AWSAFTService` papel

Essas funções são explicadas nas seções a seguir.

O AWSAFTAdmin papel, explicado

Quando você implanta o AFT, a `AWSAFTAdmin` função é criada na conta de gerenciamento do AFT. Essa função permite que o pipeline do AFT assuma a `AWSAFTExecution` função nas contas provisionadas do AWS Control Tower e do AFT, realizando, assim, ações relacionadas ao provisionamento e às personalizações da conta.

Aqui está a política embutida (artefato JSON) anexada à função: `AWSAFTAdmin`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

O artefato JSON a seguir mostra a relação de confiança da `AWSAFTAdmin` função. O número do espaço reservado `012345678901` é substituído pelo número de identificação da conta de gerenciamento da AFT.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

O AWSAFTExecution papel, explicado

Quando você implanta o AFT, a `AWSAFTExecution` função é criada nas contas de gerenciamento do AFT e do AWS Control Tower. Posteriormente, o pipeline do AFT cria a `AWSAFTExecution` função em cada conta provisionada do AFT durante o estágio de provisionamento da conta do AFT.

O AFT utiliza a `AWSControlTowerExecution` função inicialmente, para criar a `AWSAFTExecution` função em contas especificadas. A `AWSAFTExecution` função permite que o pipeline do AFT execute as etapas que são executadas durante os estágios de provisionamento e personalização da estrutura do AFT, para contas provisionadas pelo AFT e para contas compartilhadas.

> **Funções distintas ajudam você a limitar o escopo**
>
> Como prática recomendada, mantenha as permissões de personalização separadas das permissões permitidas durante a implantação inicial dos recursos. Lembre-se de que a `AWSAFTService` função se destina ao provisionamento de contas e à `AWSAFTExecution` personalização da conta. Essa separação limita o escopo das permissões permitidas durante cada fase do pipeline. Essa distinção é especialmente importante se você estiver personalizando as contas compartilhadas do AWS Control Tower, porque as contas compartilhadas podem conter informações confidenciais, como detalhes de faturamento ou informações do usuário.

Permissões para `AWSAFTExecution` função: AdministratorAccess— uma política gerenciada pela AWS

O artefato JSON a seguir mostra a política do IAM (relação de confiança) associada à `AWSAFTExecution` função. O número do espaço reservado `012345678901` é substituído pelo número de identificação da conta de gerenciamento da AFT.

Política de confiança para `AWSAFTExecution`

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

O AWSAFTService papel, explicado

A `AWSAFTService` função implanta recursos AFT em todas as contas registradas e gerenciadas, incluindo as contas compartilhadas e a conta de gerenciamento. Anteriormente, os recursos eram implantados somente pela `AWSAFTExecution` função.

A `AWSAFTService` função deve ser usada pela infraestrutura de serviços para implantar recursos durante o estágio de provisionamento, e a `AWSAFTExecution` função deve ser usada somente para implantar personalizações. Ao assumir as funções dessa forma, você pode manter um controle de acesso mais granular durante cada estágio.

Permissões para `AWSAFTService` função: AdministratorAccess— uma política gerenciada pela AWS

O artefato JSON a seguir mostra a política do IAM (relação de confiança) associada à `AWSAFTService` função. O número do espaço reservado `012345678901` é substituído pelo número de identificação da conta de gerenciamento da AFT.

Política de confiança para `AWSAFTService`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

## Serviços de componentes

Quando você implantaAFT, componentes são adicionados ao seu AWS ambiente a partir de cada um desses AWS serviços.

- AWSControl Tower — AFT usa o AWS Control Tower Account Factory na conta de gerenciamento da AWS Control Tower para provisionar contas.
- Amazon DynamoDB — cria tabelas do AFT Amazon DynamoDB na conta de gerenciamento, que armazenam solicitações de conta, histórico de auditoria de atualizações AFT da conta, metadados da conta e eventos do ciclo de vida da Control Tower. AWS AFTtambém cria gatilhos Lambda do DynamoDB para iniciar processos downstream, como iniciar o fluxo de trabalho de provisionamento de contas. AFT
- Amazon Simple Storage Service — AFT cria buckets do Amazon Simple Storage Service (S3) na conta de AFT gerenciamento e na conta de arquivamento de logs da AWS Control Tower, que armazenam os registros gerados pelos AWS serviços que o pipeline exige. AFT AFTtambém cria um bucket S3 de back-end do Terraform, nas AWS regiões primária e secundária, para armazenar os estados do Terraform gerados durante os fluxos de trabalho do pipeline. AFT
- Amazon Simple Notification Service — AFT cria tópicos do Amazon Simple Notification Service (SNS) na conta AFT de gerenciamento, que armazena notificações de sucesso e falha após o processamento de cada solicitação de AFT conta. Você pode receber essas mensagens usando o protocolo de sua escolha.
- Amazon Simple Queuing Service — AFT cria uma fila do Amazon Simple Queuing Service (AmazonSQS) na conta de FIFO gerenciamento. AFT A fila permite que você envie várias solicitações de conta em paralelo, mas envia uma solicitação por vez para a AWS Control Tower Account Factory, para processamento sequencial.
- AWS CodeBuild— AFT cria projetos de AWS CodeBuild compilação na conta AFT de gerenciamento para inicializar, compilar, testar e aplicar planos do Terraform ao AFT código-fonte em vários estágios de construção.
- AWS CodePipeline— AFT cria AWS CodePipeline pipelines na conta AFT de gerenciamento para se integrar ao seu provedor de AWS CodeStar conexões selecionado e compatível para o AFT código-fonte e para acionar trabalhos de construção. AWS CodeBuild
- AWSLambda — cria AFT funções e camadas do AWS Lambda na conta AFT de gerenciamento para realizar etapas durante os processos de solicitação, provisionamento e AFT personalização da conta.

- AWSArmazenamento de parâmetros do AWS Systems Manager — AFT configura o Armazenamento de parâmetros do Systems Manager na conta de AFT gerenciamento, para armazenar os parâmetros de configuração necessários para os processos do AFT pipeline.
- Amazon CloudWatch — AFT cria grupos de CloudWatch registros da Amazon na conta AFT de gerenciamento para armazenar registros gerados pelos AWS serviços empregados pelo AFT pipeline. O período de retenção CloudWatch dos registros está definido como`Never Expire`.
- Amazon VPC — AFT cria uma Amazon Virtual Private Cloud (VPC) para isolar serviços e recursos na conta AFT de gerenciamento em um ambiente de rede separado, para maior segurança.
- AWSKMS— AFT usa o AWS Key Management Service (KMS) na conta de AFT gerenciamento e na conta de arquivamento de registros do AWS Control Tower. AFTcria chaves para criptografar estados do Terraform, dados armazenados em tabelas e tópicos do DynamoDB. SNS Esses registros e artefatos são gerados quando AWS recursos e serviços são implantados pelo. AFT KMSas chaves criadas por AFT têm a rotação anual ativada por padrão.
- AWS Identity and Access Management (IAM) — AFT segue o modelo de privilégios mínimos recomendado. Ele cria funções e políticas de AWS Identity and Access Management (IAM) na conta AFT de gerenciamento, nas contas da AWS Control Tower e nas contas AFT provisionadas, conforme necessário, para realizar as ações necessárias durante o AFT fluxo de trabalho do pipeline.
- AWS Step Functions — AFT cria máquinas de estado do AWS Step Functions na conta AFT de gerenciamento. Essas máquinas de estado orquestram e automatizam o processo e as etapas da estrutura de provisionamento de AFT contas e das personalizações.
- Amazon EventBridge — AFT cria um barramento de EventBridge eventos da Amazon na conta de gerenciamento da AFT AWS Control Tower para capturar e armazenar eventos de longo prazo do ciclo de vida da AWS Control Tower na tabela do DynamoDB da conta AFT de gerenciamento. AFTcria regras de CloudWatch eventos da Amazon nas contas AFT de gerenciamento e gerenciamento da AWS Control Tower, que acionam várias etapas necessárias durante a execução do fluxo de trabalho do AFT pipeline
- AWS CloudTrail (Opcional) — Quando esse recurso está ativado, AFT cria uma trilha AWS CloudTrail organizacional na conta de gerenciamento da AWS Control Tower, para registrar eventos de dados para buckets do Amazon S3 e funções AWS Lambda. AFTenvia esses registros para um bucket central do S3 na conta de arquivamento de registros do AWS Control Tower.
- AWS Support (Opcional) — Quando esse recurso está ativado, AFT ativa o plano AWS Enterprise Support para contas provisionadas por. AFT Por padrão, AWS as contas são criadas com o plano AWS Basic Support ativado.

# Pipeline de provisionamento de contas AFT

Após a conclusão do estágio de provisionamento da conta do pipeline, a estrutura do AFT continua. Ele executa automaticamente uma série de etapas para garantir que as contas recém-provisionadas tenham os detalhes definidos antes do início da Personalizações da conta etapa.

Aqui estão as próximas etapas que o pipeline AFT executa.

1. Valida a entrada da solicitação da conta.
2. Recupera informações sobre a conta provisionada, por exemplo, o ID da conta.
3. Armazena os metadados da conta em uma tabela do DynamoDB na conta de gerenciamento do AFT.
4. Cria a função AWSAFTExecutiondo IAM na conta recém-provisionada. A AFT assume essa função para realizar o estágio de personalização da conta, porque essa função concede acesso ao portfólio da fábrica de contas.
5. Aplica as tags de conta que você forneceu como parte dos parâmetros de entrada da solicitação de conta.
6. Aplica as opções de recursos do AFT que você escolheu no momento da implantação do AFT.
7. Aplica as personalizações de provisionamento da conta AFT que você forneceu. A próxima seção explica mais sobre como configurar essas personalizações com uma máquina de estado do AWS Step Functions, em um `git` repositório. Às vezes, esse estágio é chamado de estágio da estrutura de provisionamento de contas. Isso faz parte do processo principal de provisionamento, mas você já configurou uma estrutura que fornece integrações personalizadas como parte do fluxo de trabalho de provisionamento de contas, antes que personalizações adicionais sejam adicionadas às contas na próxima etapa.
8. Para cada conta provisionada, ele cria uma conta AWS CodePipeline de gerenciamento do AFT, que será executada para realizar a próxima etapa (global)Personalizações da conta.
9. Invoca o pipeline de personalizações da conta para cada conta provisionada (e direcionada).
10. Envia uma notificação de sucesso ou falha para o tópico do SNS, a partir da qual você pode recuperar as mensagens.

## Configure as personalizações da estrutura de provisionamento de contas com uma máquina de estado

Se você configurar integrações personalizadas que não sejam do Terraform antes de provisionar suas contas, essas personalizações serão incluídas no fluxo de trabalho de provisionamento de contas do AFT. Por exemplo, você pode exigir determinadas personalizações para garantir que todas as contas criadas pela AFT estejam em conformidade com os padrões e políticas da sua organização, como os padrões de segurança, e esses padrões podem ser adicionados às contas antes da personalização adicional. Essas personalizações da estrutura de provisionamento de contas são implementadas em todas as contas provisionadas, antes do próximo estágio de personalização da conta global começar.

> **Note**
>
> O recurso AFT descrito nesta seção é destinado a usuários avançados que entendem o funcionamento do AWS Step Functions. Como alternativa, recomendamos que você trabalhe com os ajudantes globais no estágio de personalização da conta.

A estrutura de provisionamento de contas AFT chama uma máquina de estado do AWS Step Functions, que você define, para implementar suas personalizações. Consulte a documentação do AWS Step Functions para saber mais sobre as possíveis integrações de máquinas de estado.

Aqui estão algumas integrações comuns.

- O AWS Lambda funciona na linguagem de sua escolha
- Tarefas do AWS ECS ou AWS Fargate, usando contêineres Docker
- Atividades do AWS Step Functions usando trabalhadores personalizados, hospedados na AWS ou localmente
- Integrações com Amazon SNS ou SQS

Se nenhuma máquina de estado do AWS Step Functions for definida, o estágio passa sem operação. Para criar uma máquina de estado de personalizações de provisionamento de contas AFT, siga as instruções em. Crie sua conta AFT, provisionando, personalizações, máquina de estado Antes de adicionar personalizações, verifique se você tem os pré-requisitos em vigor.

Esses tipos de integrações não fazem parte do AWS Control Tower e não podem ser adicionados durante o estágio global de pré-API da personalização da conta AFT. Em vez disso, o pipeline AFT

permite que você configure essas personalizações como parte do processo de provisionamento, e elas são executadas no fluxo de trabalho de provisionamento. Você deve implementar essas personalizações criando sua máquina de estado com antecedência, antes de iniciar o estágio de provisionamento da conta AFT, conforme descrito nas seções a seguir.

Pré-requisitos para criar uma máquina de estado

- Um AFT totalmente implantado. Consulte Implante AWS o Control Tower Account Factory para Terraform () AFT para obter mais informações sobre a implantação do AFT.
- Configure um `git` repositório em seu ambiente para personalizações de provisionamento de contas AFT. Consulte Etapas de pós-implantação para obter mais informações.

## Crie sua conta AFT, provisionando, personalizações, máquina de estado

Etapa 1: Modificar a definição da máquina de estado

Modifique a definição de exemplo da máquina de `customizations.asl.json` estado. O exemplo está disponível no `git` repositório que você configurou para armazenar personalizações de provisionamento de contas AFT, em suas etapas de pós-implantação. Consulte o Guia do desenvolvedor do AWS Step Functions para saber mais sobre as definições de máquina de estado.

Etapa 2: incluir a configuração correspondente do Terraform

Inclua arquivos do Terraform com a `.tf` extensão no mesmo `git` repositório com a definição da máquina de estado para sua integração personalizada. Por exemplo, se você optar por chamar uma função Lambda na definição da tarefa da sua máquina de estado, inclua o `lambda.tf` arquivo no mesmo diretório. Certifique-se de incluir as funções e permissões do IAM necessárias para suas configurações personalizadas.

Quando você fornece a entrada apropriada, o pipeline do AFT invoca automaticamente sua máquina de estado e implanta suas personalizações como parte do estágio da estrutura de provisionamento de contas do AFT.

## Para reiniciar a estrutura e as personalizações de provisionamento de contas AFT

A AFT executa a estrutura de provisionamento de contas e as etapas de personalização para cada conta vendida por meio do pipeline da AFT. Para reiniciar as personalizações de provisionamento de contas, você pode usar um desses dois métodos:

1. Faça qualquer alteração em uma conta existente no repositório de solicitações de conta.

2. Provisione uma nova conta com a AFT.

# Personalizações da conta

O AFT pode implantar configurações padrão ou personalizadas em contas provisionadas. Na conta de gerenciamento da AFT, a AFT fornece um pipeline para cada conta. Com esse pipeline, você pode implementar suas personalizações em todas as contas, em um conjunto de contas ou em contas individuais. Você pode executar scripts Python, scripts bash e configurações do Terraform, ou pode interagir com a AWS CLI como parte do estágio de personalização da sua conta.

## Visão geral

Depois que suas personalizações forem especificadas nos `git` repositórios escolhidos, seja aquele em que você armazena suas personalizações globais ou onde você armazena as personalizações de sua conta, o estágio de personalização da conta é concluído automaticamente pelo pipeline do AFT. Para personalizar contas retroativamente, consulteInvoque novamente as personalizações.

Personalizações globais (opcional)

Você pode optar por aplicar determinadas personalizações a todas as contas provisionadas pela AFT. Por exemplo, se você precisar criar uma função específica do IAM ou implantar um controle personalizado em cada conta, o estágio de personalizações globais no pipeline do AFT permite que você faça isso automaticamente.

Personalizações da conta (opcional)

Para personalizar uma conta individual ou um conjunto de contas de forma diferente de outras contas provisionadas pelo AFT, você pode aproveitar a parte de personalizações de conta do pipeline do AFT para implementar configurações específicas da conta. Por exemplo, somente uma determinada conta pode exigir acesso a um gateway de internet.

## Pré-requisitos de personalização

Antes de começar a personalizar contas, verifique se esses pré-requisitos estão em vigor.

- Um AFT totalmente implantado. Para obter informações sobre como implantar, consulteConfigure e inicie sua AWS Control Tower Account Factory para Terraform.
- `git`Repositórios pré-preenchidos para personalizações globais e personalizações de contas em seu ambiente. Consulte Etapa 3: Preencher cada repositório Etapas de pós-implantação para obter mais informações.

## Aplique personalizações globais

Para aplicar personalizações globais, você deve enviar uma estrutura de pastas específica para o repositório escolhido.

- Se suas configurações personalizadas estiverem na forma de programas ou scripts em Python, coloque-as na pasta api_helpers/python em seu repositório.
- Se suas configurações personalizadas estiverem na forma de scripts Bash, coloque-as na pasta api_helpers em seu repositório.
- Se suas configurações personalizadas estiverem no formato do Terraform, coloque-as na pasta terraform em seu repositório.
- Consulte o arquivo README de personalizações globais para obter mais detalhes sobre a criação de configurações personalizadas.

> **Note**
>
> As personalizações globais são aplicadas automaticamente, após o estágio da estrutura de provisionamento da conta AFT no pipeline do AFT.

## Aplique personalizações de conta

Você pode aplicar personalizações de conta enviando uma estrutura de pastas específica para o repositório escolhido. As personalizações da conta são aplicadas automaticamente no pipeline do AFT e após o estágio global de personalizações. Você também pode criar várias pastas que contêm diferentes personalizações de conta no seu repositório de personalizações de conta. Para cada personalização de conta necessária, use as etapas a seguir.

Para aplicar personalizações de conta

1. Etapa 1: criar uma pasta para personalização de uma conta

   No repositório escolhido, copie a `ACCOUNT_TEMPLATE` pasta fornecida pelo AFT para uma nova pasta. O nome da sua nova pasta deve corresponder ao `account_customizations_name` que você forneceu na sua solicitação de conta.
2. Adicione as configurações à pasta específica de personalizações da sua conta

Você pode adicionar configurações à pasta de personalizações da sua conta com base no formato das suas configurações.

- Se suas configurações personalizadas estiverem na forma de programas ou scripts Python, coloque-as na pasta ***[account_customizations_name] /api_helpers/python que está no*** seu repositório.
- Se suas configurações personalizadas estiverem na forma de scripts Bash, coloque-as na pasta ***[account_customizations_name] /api_helpers que está no seu repositório***.
- Se suas configurações personalizadas estiverem no formato do Terraform, coloque-as na pasta ***[account_customizations_name***] /terraform que está no seu repositório.

Para obter mais informações sobre a criação de configurações personalizadas, consulte o arquivo README de personalizações da conta.

3. Consulte o **`account_customizations_name`** parâmetro específico no arquivo de solicitação de conta

   O arquivo de solicitação de conta AFT inclui o parâmetro de entrada`account_customizations_name`. Insira o nome da personalização da sua conta como o valor desse parâmetro.

> **Note**
>
> Você pode enviar várias solicitações de conta para contas em seu ambiente. Quando quiser aplicar personalizações de conta diferentes ou semelhantes, especifique as personalizações da conta usando o parâmetro de `account_customizations_name` entrada em suas solicitações de conta. Para obter mais informações, consulte Enviar várias solicitações de conta.

## Invoque novamente as personalizações

O AFT fornece uma maneira de invocar novamente as personalizações no pipeline do AFT. Esse método é útil quando você adiciona uma nova etapa de personalização ou quando está fazendo alterações em uma personalização existente. Quando você invoca novamente, o AFT inicia o pipeline de personalizações para fazer alterações na conta provisionada do AFT. Uma event-source-

based nova invocação permite que você aplique personalizações a contas individuais, a todas as contas, às contas de acordo com sua OU ou às contas selecionadas de acordo com as tags.

Siga estas três etapas para invocar novamente as personalizações para contas provisionadas pelo AFT.

Etapa 1: enviar alterações para repositórios globais ou de personalizações de **`git`** contas

Você pode atualizar suas personalizações globais e de conta conforme necessário e enviar as alterações de volta aos seus `git` repositórios. Neste momento, nada acontece. O pipeline de personalizações deve ser invocado por uma fonte de eventos, conforme explicado nas próximas duas etapas.

Etapa 2: iniciar uma execução do AWS Step Function para reinvocar personalizações

A AFT fornece uma AWS Step Function chamada `aft-invoke-customizations` na conta de gerenciamento da AFT. O objetivo dessa função é invocar novamente o pipeline de personalização para contas provisionadas pela AFT.

Aqui está um exemplo de um esquema de evento (formato JSON) que você pode criar para passar a entrada para a `aft-invoke-customizations` AWS Step Function.

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],
```

```
  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

O exemplo de esquema de eventos mostra que você pode escolher contas para incluir ou excluir do processo de reinvocação. Você pode filtrar por unidade organizacional (OU), tags de conta e ID da conta. Se você não aplicar nenhum filtro e incluir a declaração`"type":"all"`, a personalização de todas as contas provisionadas pela AFT será invocada novamente.

> **Note**
>
> Se sua versão do AWS Control Tower for 1.6.5 ou posterior, você poderá segmentar OUs aninhadas com a sintaxe). `OU Name (ou-id-1234` Para obter mais informações, consulte o tópico a seguir em GitHub.

Depois de preencher os parâmetros do evento, o Step Functions é executado e invoca as personalizações correspondentes. O AFT pode invocar no máximo 5 personalizações por vez. Step Functions espera e repete até que todas as contas que correspondem aos critérios do evento sejam concluídas.

Etapa 3: Monitore a saída do AWS Step Function e observe a CodePipeline execução da AWS

- A saída resultante do Step Function contém IDs de conta que correspondem à fonte do evento de entrada do Step Function.
- Navegue até a AWS CodePipeline em Developer Tools e veja os canais de personalização correspondentes para o ID da conta.

## Solução de problemas com o rastreamento de solicitações de personalização da conta AFT

Fluxos de trabalho de personalização de contas baseados em registros de emissão contendo AWS Lambda IDs da conta de destino e da solicitação de personalização. O AFT permite rastrear e solucionar problemas de solicitações de personalização com o Amazon CloudWatch Logs, fornecendo consultas do CloudWatch Logs Insights que você pode usar para filtrar CloudWatch os registros relacionados à sua solicitação de personalização por sua conta de destino ou ID da solicitação de personalização. Para obter mais informações, consulte Análise de dados de log com o Amazon CloudWatch Logs no Guia do usuário do Amazon CloudWatch Logs.

Para usar o CloudWatch Logs Insights para AFT

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Logs e, em seguida, escolha Logs insights.
3. Escolha Consultas.
4. Em Exemplos de consultas, escolha Account Factory for Terraform e selecione uma das seguintes consultas:

   - Registros de personalização por ID da conta

     > **Note**
     >
     > Certifique-se de substituir *“YOUR-ACCOUNT-ID” pelo ID da sua conta* de destino.

     ```
     fields @timestamp, log_message.account_id as target_account_id,
      log_message.customization_request_id as customization_request_id,
      log_message.detail as detail, @logStream
     | sort @timestamp desc
     | filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
     customization_request_id/
     ```

   - Registros de personalização por ID de solicitação de personalização

> **Note**
>
> Certifique-se de substituir *"YOUR-CUSTOMIZATION-REQUEST-ID" pelo ID da solicitação de personalização*. Você pode encontrar seu ID de solicitação de personalização na saída da máquina de estado da estrutura AWS Step Functions de provisionamento de contas AFT. Para obter mais informações sobre a estrutura de provisionamento de contas AFT, consulte Pipeline de provisionamento de contas AFT

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
```

5. Depois de selecionar uma consulta, certifique-se de selecionar um intervalo de tempo e escolha Executar consulta.

## Alternativas para controle de versão do código-fonte em AFT

AFTusa AWS CodeCommit para um sistema de controle de versão de código-fonte (VCS) e permite outros CodeConnectionsque atendam aos requisitos de seus negócios ou à arquitetura existente.

Se você estiver implantando AFT pela primeira vez e não tiver um CodeCommit repositório existente, deverá especificar um VCS provedor externo, como parte dos pré-requisitos de AFT implantação. Para obter mais informações, consulte Alternativas para controle de versão do código-fonte em AFT.

AFTsuporta as seguintes alternativas de controle de código-fonte:

- GitHub
- GitHub Servidor corporativo
- BitBucket

> **Note**
>
> Se você especificar AWS CodeCommit como seuVCS, nenhuma etapa adicional será necessária. AFTcria os `git` repositórios necessários em seu ambiente, com nomes padrão.

No entanto, você pode substituir os nomes padrão do repositório para CodeCommit, conforme necessário, estar em conformidade com seus padrões organizacionais.

## Configure um sistema alternativo de controle de versão do código-fonte (personalizadoVCS) com AFT

Para configurar um sistema alternativo de controle de versão de código-fonte para sua AFT implantação, siga estas etapas.

Etapa 1: Crie **`git`** repositórios em um sistema de controle de versão de terceiros compatível (VCS).

Se você não estiver usando AWS CodeCommit, deverá criar `git` repositórios em seu ambiente de VCS provedor AFT terceirizado compatível para os itens a seguir.

- AFTsolicitações de conta. Código de amostra disponível. Para obter mais informações sobre solicitações de AFT conta, consulteProvisionar uma nova conta com a AFT.
- AFTpersonalizações de provisionamento de contas. Código de amostra disponível. Para obter mais informações sobre personalizações de provisionamento de AFT contas, consulte. Crie sua conta AFT, provisionando, personalizações, máquina de estado
- AFTpersonalizações globais. Código de amostra disponível. Para obter mais informações sobre personalizações AFT globais, consulte. Personalizações da conta
- AFTpersonalizações da conta. Código de amostra disponível. Para obter mais informações sobre personalizações de AFT conta, consulte. Personalizações da conta

Etapa 2: Especificar os parâmetros VCS de configuração necessários para a AFT implantação

Os parâmetros de entrada a seguir são necessários para configurar seu VCS provedor como parte da AFT implantação.

- vcs_provider: Se você não estiver usando AWS CodeCommit, especifique o VCS provedor como`"bitbucket"`, ou `"github""githubenterprise"`, com base no seu caso de uso.
- github_enterprise_url: somente para clientes GitHub corporativos, especifique o. GitHub URL
- account_request_repo_name: para AWS CodeCommit usuários, esse valor é definido como. `aft-account-request` Em um ambiente AFT de VCS provedor terceirizado compatível, atualize esse valor de entrada com o nome real do seu repositório. Para BitBucket Github e GitHub Enterprise, o nome do repositório deve ter o formato. `[Org]/[Repo]`

- account_customizations_repo_name: para usuários, esse valor é definido como. AWS CodeCommit `aft-account-customizations` Em um ambiente AFT de VCS provedor terceirizado compatível, atualize esse valor de entrada com o nome do seu repositório. Para BitBucket Github e GitHub Enterprise, o nome do repositório deve ter o formato. `[Org]/[Repo]`
- account_provisioning_customizations_repo_name: para usuários, esse valor é definido como. AWS CodeCommit `aft-account-provisioning-customizations` Em um ambiente AFT de VCS provedor terceirizado compatível, atualize esse valor de entrada com o nome do seu repositório. Para BitBucket Github e GitHub Enterprise, o nome do repositório deve ter o formato. `[Org]/[Repo]`
- global_customizations_repo_name: para usuários, esse valor é definido como. AWS CodeCommit `aft-global-customizations` Em um ambiente AFT de VCS provedor terceirizado compatível, atualize esse valor de entrada com o nome do seu repositório. Para BitBucket Github e GitHub Enterprise, o nome do repositório deve ter o formato. `[Org]/[Repo]`
- account_request_repo_branch: a ramificação é `main` por padrão, mas o valor pode ser substituído.

Por padrão, AFT fontes da `main` ramificação de cada `git` repositório. Você pode substituir o valor do nome da ramificação por um parâmetro de entrada adicional. Para obter mais informações sobre os parâmetros de entrada, consulte o README arquivo no módulo AFT Terraform.

> **Para AWS CodeCommit clientes existentes**
>
> Se você criar um CodeCommit repositório com um novo nome paraAFT, poderá atualizar o nome do repositório atualizando os valores desses parâmetros de entrada.

Etapa 3: Concluir a AWS CodeStar conexão para VCS provedores terceirizados

Quando sua implantação é executada, AFT você cria os AWS CodeCommit repositórios necessários ou cria uma AWS CodeStar conexão para o VCS provedor terceirizado escolhido. No último caso, você deve entrar manualmente no console da conta AFT de gerenciamento para concluir a AWS CodeStar conexão pendente. Consulte a AWS CodeStar documentação para obter mais instruções sobre como concluir a AWS CodeStar conexão.

## Proteção de dados

O modelo de responsabilidadeAWS compartilhada se aplica à proteção de dados no AFT. Para fins de proteção de dados, recomendamos as seguintes melhores práticas de segurança.

- Siga as diretrizes de proteção de dados fornecidas pelo AWS Control Tower. Para obter detalhes, consulte Proteção de dados na AWS Control Tower.
- Preserve a configuração de estado do Terraform gerada no momento da implantação do AFT. Para obter detalhes, consulte Implante AWS o Control Tower Account Factory para Terraform () AFT.
- Alterne as credenciais confidenciais periodicamente, conforme indicado pela política de segurança da sua organização. Exemplos de segredos são tokens do Terraform, `git` tokens e assim por diante.

Criptografia em repouso

O AFT cria buckets do Amazon S3, tópicos do Amazon SNS, filas do Amazon SQS e bancos de dados do Amazon DynamoDB que são criptografados em repouso com chaves do Key Management Service. AWS As chaves KMS criadas pelo AFT têm a rotação anual ativada por padrão. Se você escolher as distribuições Terraform Cloud ou Terraform Enterprise do Terraform, o AFT incluirá um SecureString parâmetro AWS Systems Manager para armazenar valores de token do Terraform que são confidenciais.

O AFT usa AWS serviços descritos em Serviços de componentes que, por padrão, são criptografados em repouso. Para obter detalhes, consulte a AWS documentação de cada AWS serviço componente do AFT e conheça as práticas de proteção de dados seguidas por cada serviço.

Criptografia em trânsito

A AFT depende dos AWS serviços descritos em Serviços de componentes que, por padrão, empregam criptografia em trânsito. Para obter detalhes, consulte a AWS documentação de cada AWS serviço componente do AFT e conheça as práticas de proteção de dados seguidas por cada serviço.

Para distribuições do Terraform Cloud ou do Terraform Enterprise, o AFT chama uma API de endpoint HTTPS para acessar sua organização do Terraform. Se você escolher um provedor de VCS terceirizado suportado por AWS CodeStar conexões, o AFT chamará uma API de endpoint HTTPS para acessar sua organização provedora de VCS.

## Remover uma conta do AFT

Este tópico descreve como remover uma conta do AFT para que o pipeline do AFT pare de implantar e atualizar a conta.

> **Important**
>
> A remoção de uma conta do pipeline AFT é irreversível e pode resultar em perda de estado.

Você pode remover uma conta do AFT quando quiser fechar a conta de um aplicativo retirado, isolar uma conta comprometida ou mover uma conta de uma organização para outra.

> **Note**
>
> Remover uma conta do AFT é diferente de excluir uma conta do AWS Control Tower ou Conta da AWS. Quando você remove uma conta do AFT, o AWS Control Tower ainda gerencia a conta. Para excluir uma conta do AWS Control Tower ou Conta da AWSconsulte o seguinte:
>
> - Desgerencie uma conta no Guia do usuário do AWS Control Tower.
> - Fechar uma conta no GuiaAWS Billing do usuário.

Para remover uma conta dos pipelines do AFT

O procedimento a seguir descreve como remover uma conta do AFT.

1. Remover conta do **`git`** repositório que armazena solicitações de conta

   No `git` repositório em que você armazena as solicitações de conta, exclua a solicitação de conta da conta que você deseja remover do AFT.

   Quando você remove uma solicitação de conta do repositório de solicitações de conta, o AFT exclui o pipeline de personalização e os metadados da conta. Para obter mais informações, consulte as notas de versão 1.8.0 do AFT on. GitHub
2. Exclua o espaço de trabalho do Terraform (somente para clientes do Terraform Cloud e do Terraform Enterprise)

   Exclua as personalizações globais e os espaços de trabalho de personalizações de conta da conta que você deseja remover do AFT.
3. Exclua o estado do Terraform do back-end do Amazon S3

Na conta de gerenciamento do AFT, exclua todas as pastas relevantes dentro dos buckets do Amazon S3 para a conta que você deseja remover do AFT.

> **Tip**
>
> Nos exemplos a seguir, `012345678901` substitua pelo número de ID da conta de gerenciamento AFT.

Exemplo: Terraform OSS

Ao escolher o Terraform OSS, você encontra 3 pastas para cada conta nos buckets `aft-backend-012345678901-primary-region` e no Amazon `aft-backend-012345678901-secondary-region` S3. Essas pastas estão relacionadas ao estado das personalizações da conta, ao estado do pipeline de personalizações e ao estado das personalizações globais.

Exemplo: Terraform Cloud ou Terraform Enterprise

Ao escolher o Terraform Cloud ou o Terraform Enterprise, você encontra uma pasta para cada conta nos buckets `aft-backend-012345678901-primary-region` e no Amazon `aft-backend-012345678901-secondary-region` S3. Essas pastas estão relacionadas ao estado do pipeline de personalizações.

## Métricas operacionais

Por padrão, o Account Factory for Terraform (AFT) envia métricas operacionais anônimas para o. AWSUsamos esses dados para entender como os clientes estão usando o AFT para que possamos melhorar a qualidade e os recursos da solução. Você pode cancelar a coleta de dados alterando um parâmetro durante a implantação do AFT. Quando a coleta é ativada, os seguintes dados são enviados para AWS:

- Solução: O identificador específico do AFT
- Versão: A versão do AFT
- Identificador exclusivo universal (UUID): identificador exclusivo gerado aleatoriamente para cada implantação do AFT
- Carimbo de data e hora: data e hora da coleta de dados

- Dados: configuração do AFT e ações tomadas pelo cliente

AWS possui os dados coletados. A coleta de dados está sujeita à AWS Política de Privacidade.

> **Note**
>
> As versões do AFT anteriores à 1.6.0 não relatam métricas de uso a. AWS

Para optar por não receber métricas de relatórios:

- Defina o valor de entrada de `aft_metrics_reporting` to `false` em seu arquivo de configuração de entrada do Terraform, conforme mostrado no exemplo a seguir, e reimplante o AFT. Esse valor é definido como `true` por padrão, se você não o definir explicitamente.

Se você copiar o exemplo, lembre-se de substituir seus valores reais de ID e região pelos itens fornecidos em strings porx.

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

## Guia de solução de problemas do Account Factory for Terraform (AFT)

Esta seção pode ajudá-lo a solucionar problemas comuns que você pode encontrar ao usar o Account Factory for Terraform (AFT).

Tópicos

## Problemas gerais

- Cotas de AWS recursos excedidas

  Se seus grupos de registros indicarem que você excedeu as cotas de AWS recursos, entre em contato com o Support AWS . O Account Factory usa Serviços da AWS com cotas de recursos que incluem AWS CodeBuild AWS Organizations, e. AWS Systems Manager Para mais informações, consulte:

  - O que é AWS CodeBuild? no Guia do CodeBuild usuário.
  - O que é AWS Organizations? no Guia do Usuário do Organizations.
  - O que é AWS Systems Manager? no Guia do usuário do Systems Manager.
- Versão desatualizada do Account Factory

  Se você encontrar um problema e achar que o problema é um bug, verifique se você tem a versão mais recente do Account Factory. Para obter mais informações, consulte Atualizando a versão Account Factory.
- Foram feitas alterações locais no código-fonte do Account Factory

  Account Factory é um projeto de código aberto. O AWS Control Tower é compatível com o código principal do Account Factory. Se você fizer uma alteração local no código principal do Account Factory, o AWS Control Tower só suportará sua implantação do Account Factory com base no melhor esforço.
- Permissões de função insuficientes do Account Factory

  O Account Factory cria funções e políticas do IAM para gerenciar implantações e personalizações de contas vendidas. Se você alterar essas funções ou políticas, o pipeline do Account Factory pode não conseguir realizar determinadas ações. Para obter mais informações, consulte Funções obrigatórias.
- Repositórios de contas não preenchidos corretamente

  Certifique-se de seguir as etapas de pós-implantação antes de provisionar as contas.

- Não é detectado o desvio após alterar a OU manualmente

> **Note**
>
> O AWS Control Tower detecta o desvio automaticamente. Para obter informações sobre como resolver desvios, consulte Detectar e resolver desvios no AWS Control Tower.

O desvio não é detectado quando a unidade organizacional (OU) é alterada manualmente. Isso se deve à natureza orientada por eventos do Account Factory. Quando uma solicitação de conta é enviada, o recurso que o Terraform gerencia é um item do Amazon DynamoDB, não uma conta direta. Depois que um item é alterado, a solicitação é colocada em uma fila, onde o AWS Control Tower a processa por meio do Service Catalog (o serviço que gerencia os detalhes da conta). Se você alterar a OU manualmente, o desvio não será detectado porque a solicitação da conta não foi alterada.

## Problemas relacionados ao provisionamento/registro da conta

- A solicitação de conta (endereço de e-mail/nome) já existe

  O problema geralmente resulta em uma falha do produto Service Catalog durante o provisionamento ou como. `ConditionalCheckFailedException`

  Você pode encontrar mais informações sobre o problema fazendo o seguinte:

  - Revise seus grupos de registros do Terraform ou do CloudWatch Logs.
  - Analise as falhas que são emitidas para o tópico do Amazon SNS`aft-failure-notifications`.
- Solicitação de conta malformada

  Certifique-se de que sua solicitação de conta siga o esquema esperado. Para ver exemplos, consulte terraform-aws-control_tower_account_factory em. GitHub
- Cotas de recursos excedidas da AWS Organizations

  Certifique-se de que sua solicitação de conta não exceda as cotas AWS Organizations de recursos. Para obter mais informações, consulte Quotas for AWS Organizations.

## Problemas relacionados à invocação de personalizações

- Conta de destino não integrada ao Account Factory

  Certifique-se de que todas as contas incluídas em uma solicitação de personalização tenham sido integradas ao Account Factory. Para obter mais informações, consulte Atualizar uma conta existente.

- Conta que os destinos da solicitação de personalização existem na **`aft-request-metadata`** tabela do DynamoDB, mas não no repositório de solicitações de conta

  Formate sua solicitação de invocação de personalização para excluir a conta ofensiva fazendo o seguinte:

  - Na `aft-request-metadata` tabela do DynamoDB, exclua a entrada que faz referência à conta que não está mais no seu repositório de solicitações de conta.
  - Não usar “todos” como alvo.
  - Não tem como alvo a OU à qual a conta pertence.
  - Não segmentar diretamente a conta.

- Usou o token incorreto para o Terraform Cloud

  Certifique-se de configurar o token correto. O Terraform Cloud suporta apenas tokens baseados em equipe, não tokens baseados em organização.

- Falha ao criar a conta antes da criação do pipeline de personalização da conta; não é possível personalizar a conta

  Faça uma alteração na especificação da conta no repositório de solicitações de conta. Quando você faz uma alteração, como alterar o valor de uma tag para uma conta, o Account Factory segue o caminho que tenta criar o pipeline, mesmo que ele não exista.

## Problemas relacionados ao fluxo de trabalho de personalização da conta

Se você estiver enfrentando problemas relacionados ao fluxo de trabalho de personalização da conta, certifique-se de que sua versão do AFT seja 1.8.0 ou superior e exclua todas as instâncias de metadados relacionados à conta da tabela de solicitações do DynamoDB.

Para obter informações sobre a versão 1.8.0 do AFT, consulte a versão 1.8.0 ativada. GitHub

Para obter informações sobre como verificar e atualizar sua versão do AFT, consulte o seguinte:

- Verifique a versão AFT
- Atualize a versão AFT

Você também pode rastrear e solucionar problemas de solicitações de personalização usando as consultas do Amazon CloudWatch Logs Insights para filtrar registros contendo sua conta de destino e IDs de solicitação de personalização. Para obter mais informações, consulte Solução de problemas com o rastreamento de solicitações de personalização da conta AFT.

# Detecte e resolva desvios na AWS Control Tower

Identificar e resolver desvios é uma tarefa operacional regular para administradores de contas de gerenciamento da AWS Control Tower. Resolver o desvio ajuda a garantir sua conformidade com os requisitos de governança.

Quando você cria sua zona de pouso, a zona de pouso e todas as unidades organizacionais (OUs), contas e recursos estão em conformidade com as regras de governança impostas pelos controles escolhidos. À medida que você e os membros da sua organização usam o landing zone, mudanças nesse status de conformidade podem ocorrer. Algumas mudanças podem ser acidentais e algumas podem ser feitas intencionalmente para responder a eventos operacionais sensíveis ao tempo.

A detecção de oscilações ajuda a identificar recursos que precisam de alterações ou atualizações de configuração para resolver a oscilação.

## Detectando deriva

AWSO Control Tower detecta o desvio automaticamente. Para detectar desvios, a `AWSControlTowerAdmin` função exige acesso persistente à sua conta de gerenciamento para que a AWS Control Tower possa fazer chamadas somente para leitura API para. AWS Organizations Essas API chamadas aparecem como AWS CloudTrail eventos.

O Drift aparece nas notificações do Amazon Simple Notification Service SNS (Amazon) que são agregadas na conta de auditoria. As notificações em cada conta de membro enviam alertas para um SNS tópico local da Amazon e para uma função Lambda.

Para controles que fazem parte do AWS Security Hub Service-Managed Standard: AWS Control Tower, o desvio é mostrado nas páginas Conta e Detalhes da Conta no console da AWS Control Tower, bem como por meio de uma notificação da Amazon. SNS

Os administradores de contas de membros podem (e, como melhor prática, devem) assinar as notificações de SNS deriva de contas específicas. Por exemplo, o `aws-controltower-AggregateSecurityNotifications` SNS tópico fornece notificações de deriva. O console AWS Control Tower indica aos administradores da conta de gerenciamento quando ocorreu um desvio. Para obter mais informações sobre SNS tópicos para detecção e notificação de desvios, consulte Prevenção e notificação de desvios.

Eliminação da duplicação de notificações do Drift

Se o mesmo tipo de desvio ocorrer no mesmo conjunto de recursos várias vezes, o AWS Control Tower enviará uma SNS notificação somente para a instância inicial do desvio. Se a AWS Control Tower detectar que essa instância de desvio foi corrigida, ela enviará outra notificação somente se o desvio ocorrer novamente para esses recursos idênticos.

Exemplos: desvios e SCP desvios de contas são tratados da seguinte maneira

- Se você modificar o mesmo gerenciado SCP várias vezes, receberá uma notificação na primeira vez em que o modificar.
- Se você modificar um desvio gerenciadoSCP, depois remediar o desvio e modificá-lo novamente, receberá duas notificações.
- Se uma conta for movida entre a mesma origem e o mesmo destino OUs várias vezes, sem primeiro reparar o desvio, uma única notificação será enviada, mesmo que a conta tenha sido movida entre elas OUs mais de uma vez.

Tipos de desvio de conta

- Conta movida entre OUs
- Conta removida da organização

> **Note**
>
> Quando você move uma conta de uma OU para outra, os controles da OU anterior não são removidos. Se você habilitar qualquer novo controle baseado em gancho na OU de destino, o antigo o controle baseado em gancho é removido da conta e o novo controle o substitui. Os controles implementados com AWS Config regras SCPs e regras sempre devem ser removidos manualmente quando uma conta é alteradaOUs.

Tipos de mudança de política

- SCPatualizado
- SCPanexado à OU
- SCPseparado da OU
- SCPanexado à conta

Para obter mais informações, consulte Tipos de deriva de governança.

## Resolvendo o desvio

Embora a detecção seja automática, as etapas para resolver oscilações devem ser feitas por meio do console.

- Muitos tipos de deriva podem ser resolvidos por meio da página de configurações da zona de pouso. Você pode escolher o botão Redefinir na seção Versões para resolver esses tipos de desvio.
- Se sua OU tiver menos de 1.000 contas, você poderá resolver o desvio nas contas provisionadas pelo Account Factory, ou o SCP desvio, selecionando Registrar UO novamente na página Organização ou na página de detalhes da OU.
- Talvez você consiga resolver o desvio de contas, por exemploConta-membro migrada, atualizando uma conta individual. Para obter mais informações, consulte Atualize a conta no console.

⚠ Quando você toma medidas para resolver o desvio em uma versão de landing zone, dois comportamentos são possíveis.

- Se você estiver usando a versão mais recente da zona de pouso, ao escolher Redefinir e depois escolher Confirmar, os recursos da zona de pouso derivada serão redefinidos para a configuração salva da AWS Control Tower. A versão landing zone permanece a mesma.
- Se você não estiver usando a versão mais recente, deverá escolher Atualizar. A zona de pouso foi atualizada para a versão mais recente da zona de pouso. O desvio é resolvido como parte desse processo.

## Considerações sobre desvios e varreduras SCP

AWSO Control Tower escaneia seu gerente SCPs diariamente para verificar se os controles correspondentes foram aplicados corretamente e se não foram desviados. Para recuperá-los SCPs e verificá-los, o AWS Control Tower liga AWS Organizations em seu nome, usando uma função em sua conta de gerenciamento.

Se um escaneamento da AWS Control Tower descobrir um desvio, você receberá uma notificação. AWSO Control Tower envia apenas uma notificação por problema de deriva. Portanto, se sua landing

zone já estiver em um estado de deriva, você não receberá notificações adicionais a menos que um novo item de deriva seja encontrado.

AWS Organizations limita a frequência com que cada um deles APIs pode ser chamado. Esse limite é expresso em transações por segundo (TPS) e é conhecido como TPSlimite, taxa de limitação ou taxa de API solicitação. Quando a AWS Control Tower audita sua SCPs chamada AWS Organizations, as API chamadas que a AWS Control Tower faz são contabilizadas em seu TPS limite, porque a AWS Control Tower usa a conta de gerenciamento para fazer as chamadas.

Em raras situações, esse limite pode ser atingido quando você chama o mesmo APIs repetidamente, seja por meio de uma solução de terceiros ou de um script personalizado que você escreveu. Por exemplo, se você e a AWS Control Tower ligarem da mesma forma AWS Organizations APIs no mesmo momento (dentro de 1 segundo) e os TPS limites forem atingidos, as chamadas subsequentes serão limitadas. Ou seja, essas chamadas retornam um erro como`Rate exceeded`.

Se uma taxa de API solicitação for excedida

- Se a AWS Control Tower atingir o limite e for limitada, pausaremos a execução da auditoria e a retomaremos posteriormente.
- Se sua carga de trabalho atingir o limite e for limitada, o resultado pode variar de uma leve latência até um erro fatal na carga de trabalho, dependendo de como a carga de trabalho está configurada. Esse caso extremo é algo que você deve conhecer.

Uma SCP verificação diária consiste em

1. Recuperando seu recém-ativoOUs.
2. Para cada OU registrada, recuperando todas SCPs gerenciadas pela AWS Control Tower que estão conectadas à OU. SCPsOs gerenciados têm identificadores que começam com`aws-guardrails`.
3. Para cada controle preventivo habilitado na OU, verificando se a declaração de política do controle está presente na UO gerenciadaSCPs.

Uma OU pode ter um ou mais gerenciadosSCPs.

# Tipos de desvio a serem resolvidos imediatamente

A maioria dos tipos de oscilações pode ser resolvida pelos administradores. Alguns tipos de deriva devem ser resolvidos imediatamente, incluindo a exclusão de uma unidade organizacional exigida pela zona de pouso da AWS Control Tower. Aqui estão alguns exemplos de grandes desvios que você pode evitar:

- Não exclua a OU de segurança: a unidade organizacional originalmente chamada de Segurança durante a configuração da landing zone pela AWS Control Tower não deve ser excluída. Se você excluí-lo, você verá uma mensagem de erro instruindo você a redefinir a landing zone imediatamente. Você não poderá realizar nenhuma outra ação na AWS Control Tower até que a reinicialização seja concluída.
- Não exclua as funções necessárias: o AWS Control Tower verifica determinadas funções AWS Identity and Access Management (IAM) quando você faz login no console para verificar se há IAMvariação de funções. Se essas funções estiverem ausentes ou inacessíveis, você verá uma página de erro instruindo você a redefinir sua landing zone. Essas funções são `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRoleAWSControlTowerStackSetRole`.

  Para obter mais informações sobre essas funções, consultePermissões necessárias para usar o console do AWS Control Tower.
- Não exclua todos os adicionaisOUs: se você excluir a unidade organizacional originalmente chamada Sandbox durante a configuração da zona de pouso pela AWS Control Tower, sua zona de pouso ficará em um estado de deriva, mas você ainda poderá usar a AWS Control Tower. É necessária pelo menos uma OU adicional para que a AWS Control Tower opere, mas não precisa ser a OU Sandbox.
- Não remova contas compartilhadas: se você remover contas compartilhadas do FoundationalOUs, como remover a conta de registro da OU de segurança, sua landing zone ficará em um estado de desvio. A landing zone deve ser redefinida para que você possa continuar usando o console AWS Control Tower.

# Mudanças reparáveis nos recursos

Aqui está uma lista de alterações nos recursos da AWS Control Tower que são permitidas, embora elas criem um desvio solucionável. Os resultados dessas operações permitidas podem ser vistos no console do AWS Control Tower, embora uma atualização possa ser necessária.

Para obter mais informações sobre como resolver o desvio resultante, consulte Managing Resources Outside of AWS Control Tower.

Alterações permitidas fora do console AWS Control Tower

- Altere o nome de uma OU registrada.
- Altere o nome da OU de segurança.
- Altere o nome das contas dos membros em Não fundacionalOUs.
- Altere o nome das contas compartilhadas do AWS Control Tower na UO de Segurança.
- Exclua uma OU não fundamental.
- Exclua uma conta inscrita de uma OU não básica.
- Altere o endereço de e-mail de uma conta compartilhada na OU de segurança.
- Altere o endereço de e-mail de uma conta de membro em uma OU registrada.

> **Note**
>
> A transferência de contas entre contas OUs é considerada um desvio e deve ser resolvida.

## Oscilação e provisionamento de contas

Se sua landing zone estiver em um estado de deriva, o recurso Inscrever conta no AWS Control Tower não funcionará. Nesse caso, você deve provisionar novas contas por meio do AWS Service Catalog. Para obter instruções, consulte Provisionar contas com AWS Service Catalog Account Factory .

Em particular, se você fez determinadas alterações em suas contas por meio do Service Catalog, como alterar o nome do seu portfólio, o recurso Inscrever conta não funcionará.

## Tipos de oscilação de governança

O desvio de governança, também chamado de desvio organizacional, ocorre quandoOUs,SCPs, e as contas dos membros são alteradas ou atualizadas. Os tipos de desvio de governança que podem ser detectados no AWS Control Tower são os seguintes:

- Conta-membro migrada

- Conta-membro removida
- Atualização não planejada para gerenciada SCP
- SCPAnexado à conta do membro
- SCPAnexado à OU gerenciada
- SCPSeparado da OU gerenciada
- OU básica excluída
- Desvio de controle do Security Hub
- Acesso confiável desativado

Outro tipo de deriva é a deriva da landing zone, que pode ser encontrada na conta de gerenciamento. A variação da zona de destino consiste em uma mudança de IAM função ou qualquer tipo de mudança organizacional que afete especificamente as contas básicas OUs e compartilhadas.

Um caso especial de deriva na zona de pouso é a deriva de função, que é detectada quando uma função necessária não está disponível. Se esse tipo de desvio ocorrer, o console exibirá uma página de aviso e algumas instruções sobre como restaurar a função. Sua landing zone não estará disponível até que a mudança de função seja resolvida. Para obter mais informações sobre o drift, consulte Não exclua as funções necessárias na seção chamadaTipos de desvio a serem resolvidos imediatamente.

AWSA Control Tower não se preocupa com outros serviços que funcionam com a conta de gerenciamento, incluindo, CloudTrail CloudWatch, IAM Identity Center,, AWS CloudFormation AWS Config, e assim por diante. Nenhuma detecção de desvios está disponível em contas infantis, porque essas contas são protegidas por controles preventivos obrigatórios.

No entanto, ele relata desvios em relação aos controles que fazem parte do Padrão AWS Security Hub Gerenciado de Serviços: Control Tower AWS.

## Conta-membro migrada

Esse tipo de desvio ocorre na conta e não na OU. Esse tipo de desvio pode ocorrer quando uma conta de membro da AWS Control Tower, a conta de auditoria ou a conta de arquivamento de registros é movida de uma OU da AWS Control Tower registrada para qualquer outra OU. A seguir está um exemplo da SNS notificação da Amazon quando esse tipo de desvio é detectado.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 1000 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

## Soluções

Quando esse tipo de desvio ocorre em uma conta provisionada pelo Account Factory em uma OU com até 1.000 contas, você pode resolvê-lo da seguinte maneira:

- Navegando até a página Organização no console do AWS Control Tower, selecionando a conta e escolhendo Atualizar conta no canto superior direito (opção mais rápida para contas individuais).
- Navegue até a página Organização no console do AWS Control Tower e escolha Registrar novamente na OU que contém a conta (opção mais rápida para várias contas). Para obter mais informações, consulte Registre uma unidade organizacional existente na AWS Control Tower.
- Atualização do produto provisionado no Account Factory. Para obter mais informações, consulte Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog.

  > **Note**
  >
  > Se você tiver várias contas individuais para atualizar, veja também este método para fazer atualizações com um script:Provisione e atualize contas usando automação.

- Quando esse tipo de desvio ocorre em uma OU com mais de 1000 contas, a resolução do desvio pode depender do tipo de conta que foi movida, conforme explicado nos próximos parágrafos. Para obter mais informações, consulte Atualize sua landing zone.

- Se uma conta provisionada pelo Account Factory for movida — Em uma OU com menos de 1.000 contas, você pode resolver o desvio da conta atualizando o produto provisionado no Account Factory, registrando novamente a OU ou atualizando sua landing zone.

  Em uma OU com mais de 1.000 contas, você deve resolver o problema fazendo uma atualização em cada conta movida, seja por meio do console AWS Control Tower ou do produto provisionado, pois o novo registro da OU não executará a atualização. Para obter mais informações, consulte Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog.
- Se uma conta compartilhada for movida, você pode resolver o problema de mover a conta de auditoria ou arquivamento de registros atualizando sua landing zone. Para obter mais informações, consulte Atualize sua landing zone.

⚠ Nome do campo obsoleto

O nome do campo `MasterAccountID` foi alterado `ManagementAccountID` para estar em conformidade com AWS as diretrizes. O nome antigo está obsoleto. A partir de 2022, os scripts que contêm o nome do campo obsoleto não funcionarão mais.

## Conta-membro removida

Esse tipo de desvio pode ocorrer quando a conta de um membro é removida de uma unidade organizacional registrada da AWS Control Tower. O exemplo a seguir mostra a SNS notificação da Amazon quando esse tipo de desvio é detectado.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
```

```
}
```

### Resolução

- Quando esse tipo de desvio ocorre em uma conta de membro, você pode resolver o desvio atualizando a conta no console AWS Control Tower ou no Account Factory. Por exemplo, você pode adicionar a conta a outra OU registrada a partir do assistente de atualização do Account Factory. Para obter mais informações, consulte Atualize e mova contas de fábrica de contas com o AWS Control Tower ou com AWS Service Catalog.
- Se uma conta compartilhada for removida de uma OU Foundational, você deverá resolver o desvio redefinindo sua landing zone. Até que esse desvio seja resolvido, você não poderá usar o console AWS Control Tower.
- Para obter mais informações sobre como resolver o desvio de contas eOUs, consulte. Se você gerencia recursos fora do AWS Control Tower

> **Note**
>
> No Service Catalog, o produto provisionado pelo Account Factory que representa a conta não é atualizado para remover a conta. Em vez disso, o produto provisionado é exibido como `TAINTED` e em um estado de erro. Para limpar, acesse o Service Catalog, escolha o produto provisionado e, em seguida, escolha Terminate.

## Atualização não planejada para gerenciada SCP

Esse tipo de desvio pode ocorrer quando um controle SCP de um é atualizado no AWS Organizations console ou programaticamente usando o AWS CLI ou um dos. AWS SDKs A seguir está um exemplo da SNS notificação da Amazon quando esse tipo de desvio é detectado.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
```

```
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

### Resolução

Quando esse tipo de desvio ocorre em uma OU com até 1.000 contas, você pode resolvê-lo da seguinte forma:

- Navegar até a página Organização no console do AWS Control Tower para registrar novamente a OU (opção mais rápida). Para obter mais informações, consulte Registre uma unidade organizacional existente na AWS Control Tower.
- Atualizando sua landing zone (opção mais lenta). Para obter mais informações, consulte Atualize sua landing zone.

Quando esse tipo de desvio ocorrer em uma OU com mais de 1000 contas, resolva-o atualizando sua landing zone. Para obter mais informações, consulte Atualize sua landing zone.

## SCPAnexado à OU gerenciada

Esse tipo de desvio pode ocorrer quando um controle SCP for conectado a qualquer outra UO. Essa ocorrência é especialmente comum quando você está trabalhando em seu computador OUs de fora do console AWS Control Tower. A seguir está um exemplo da SNS notificação da Amazon quando esse tipo de desvio é detectado.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
```

```
}
```

### Resolução

Quando esse tipo de desvio ocorre em uma OU com até 1.000 contas, você pode resolvê-lo da seguinte forma:

- Navegar até a página Organização no console do AWS Control Tower para registrar novamente a OU (opção mais rápida). Para obter mais informações, consulte Registre uma unidade organizacional existente na AWS Control Tower.
- Atualizando sua landing zone (opção mais lenta). Para obter mais informações, consulte Atualize sua landing zone.

Quando esse tipo de desvio ocorrer em uma OU com mais de 1000 contas, resolva-o atualizando sua landing zone. Para obter mais informações, consulte Atualize sua landing zone.

## SCPSeparado da OU gerenciada

Esse tipo de desvio pode ocorrer quando um controle SCP for separado de uma OU gerenciada pela AWS Control Tower. Essa ocorrência é especialmente comum quando você está trabalhando fora do console do AWS Control Tower. A seguir está um exemplo da SNS notificação da Amazon quando esse tipo de desvio é detectado.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

### Resolução

Quando esse tipo de desvio ocorre em uma OU com até 1.000 contas, você pode resolvê-lo da seguinte forma:

- Navegar até a OU no console AWS Control Tower para registrar novamente a OU (opção mais rápida). Para obter mais informações, consulte Registre uma unidade organizacional existente na AWS Control Tower.
- Atualizando sua landing zone (opção mais lenta). Se o desvio estiver afetando um controle obrigatório, o processo de atualização cria uma nova política de controle de serviço (SCP) e a anexa à OU para resolver o desvio. Para obter mais informações sobre como atualizar sua landing zone, consulteAtualize sua landing zone.

Quando esse tipo de desvio ocorrer em uma OU com mais de 1000 contas, resolva-o atualizando sua landing zone. Se o desvio estiver afetando um controle obrigatório, o processo de atualização cria uma nova política de controle de serviço (SCP) e a anexa à OU para resolver o desvio. Para obter mais informações sobre como atualizar sua landing zone, consulteAtualize sua landing zone.

## SCPAnexado à conta do membro

Esse tipo de desvio pode ocorrer quando um controle SCP for anexado a uma conta no console Organizations. As grades de proteção e suas SCPs podem ser ativadas OUs (e, portanto, aplicadas a todas as contas inscritas de uma OU) por meio do console AWS Control Tower. A seguir está um exemplo da SNS notificação da Amazon quando esse tipo de desvio é detectado.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

### Resolução

Esse tipo de desvio ocorre na conta e não na OU.

Quando esse tipo de desvio ocorre para contas em uma OU básica, como a OU de segurança, a resolução é atualizar sua landing zone. Para obter mais informações, consulte Atualize sua landing zone.

Quando esse tipo de desvio ocorre em uma OU não básica com até 1.000 contas, você pode resolvê-lo da seguinte forma:

- Separar a AWS Control Tower SCP da conta de fábrica da conta.
- Navegar até a OU no console AWS Control Tower para registrar novamente a OU (opção mais rápida). Para obter mais informações, consulte Registre uma unidade organizacional existente na AWS Control Tower.

Quando esse tipo de desvio ocorre em uma OU com mais de 1.000 contas, você pode tentar resolvê-lo atualizando a configuração de fábrica da conta. Talvez não seja possível resolvê-lo com sucesso. Para obter mais informações, consulte Atualize sua landing zone.

## OU básica excluída

Esse tipo de desvio se aplica somente à AWS Control Tower FoundationalOUs, como a Security OU. Isso pode ocorrer se uma OU Foundational for excluída fora do console do AWS Control Tower. O Foundational OUs não pode ser movido sem criar esse tipo de desvio, porque mover uma OU é o mesmo que excluí-la e adicioná-la em outro lugar. Quando você resolve o desvio atualizando sua landing zone, o AWS Control Tower substitui o Foundational OU no local original. O exemplo a seguir mostra uma SNS notificação da Amazon que você pode receber quando esse tipo de desvio for detectado.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
```

```
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

### Resolução

Como esse desvio ocorre OUs somente para o Foundational, a resolução é atualizar a landing zone. Quando outros tipos de OUs são excluídos, o AWS Control Tower é atualizado automaticamente.

Para obter mais informações sobre como resolver o desvio de contas eOUs, consulte. Se você gerencia recursos fora do AWS Control Tower

## Desvio de controle do Security Hub

Esse tipo de desvio ocorre quando um controle que faz parte do AWS Security Hub Service-Managed Standard: AWS Control Tower relata um estado de desvio. O AWS Security Hub serviço em si não relata um estado de desvio para esses controles. Em vez disso, o serviço envia suas descobertas para a AWS Control Tower.

O desvio de controle do Security Hub também pode ser detectado se a AWS Control Tower não receber uma atualização de status do Security Hub em mais de 24 horas. Se essas descobertas não forem recebidas conforme o esperado, a AWS Control Tower verifica se o controle está em desvio. O exemplo a seguir mostra uma SNS notificação da Amazon que você pode receber quando esse tipo de desvio for detectado.

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
```

```
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

### Resolução

Para OUs com menos de 1000 contas, a solução é registrar novamente a OU, o que redefine o controle para o estado original. Para qualquer UO, você pode remover e reativar o controle por meio do console ou da AWS Control TowerAPIs, que também redefine o controle.

Para obter mais informações sobre como resolver o desvio de contas eOUs, consulte. Se você gerencia recursos fora do AWS Control Tower

## Acesso confiável desativado

Esse tipo de deriva se aplica às zonas de pouso da AWS Control Tower. Isso ocorre quando você desativa o acesso confiável à AWS Control Tower AWS Organizations depois de configurar sua zona de pouso da AWS Control Tower.

Quando o acesso confiável é desativado, a AWS Control Tower não recebe mais eventos de alteração de AWS Organizations. AWSA Control Tower depende desses eventos de mudança para se manter sincronizada com. AWS Organizations Como resultado, a AWS Control Tower pode perder mudanças organizacionais nas contas OUs e. É por isso que é importante registrar novamente cada OU, sempre que você atualizar sua landing zone.

Exemplo: SNS notificação da Amazon

Veja a seguir um exemplo da SNS notificação da Amazon que você recebe quando esse tipo de desvio ocorre.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

### Resolução

AWSO Control Tower notifica você quando esse tipo de desvio ocorre no console da AWS Control Tower. A resolução é redefinir sua zona de pouso da AWS Control Tower. Para obter mais informações, consulte Resolvendo o desvio.

## Se você gerencia recursos fora do AWS Control Tower

O AWS Control Tower configura contas, unidades organizacionais e outros recursos em seu nome, mas você é o proprietário desses recursos. Você pode alterar esses recursos dentro ou fora do AWS Control Tower. O local mais comum para alterar recursos fora do AWS Control Tower é o AWS Organizations console. Este tópico descreve como reconciliar alterações nos recursos da AWS Control Tower quando você faz as alterações fora da AWS Control Tower.

Renomear, excluir e mover recursos para fora do console do AWS Control Tower faz com que o console fique fora de sincronia. Muitas mudanças podem ser reconciliadas automaticamente. Certas mudanças exigem uma redefinição na sua landing zone para atualizar as informações exibidas no console do AWS Control Tower.

Em geral, as alterações que você faz fora do console do AWS Control Tower nos recursos da AWS Control Tower criam um estado de desvio solucionável em sua landing zone. Para mais informações sobre essas alterações, consulte Mudanças reparáveis nos recursos.

Tarefas que exigem redefinição da zona de pouso

- Excluindo a OU de segurança (um caso especial, que não deve ser feito levianamente).
- Remover uma conta compartilhada da OU de segurança (não recomendado).
- Atualizar, anexar ou desanexar um SCP associado à OU de segurança.

Alterações que são atualizadas automaticamente pelo AWS Control Tower

- Alterar o endereço de e-mail de uma conta registrada
- Renomear uma conta registrada
- Criação de uma nova unidade organizacional (OU) de nível superior
- Renomeando uma OU registrada
- Excluindo uma OU registrada (exceto a OU de segurança, que requer uma atualização).
- Excluindo uma conta inscrita (exceto uma conta compartilhada na OU de segurança)

> **Note**
>
> AWS Service Catalog lida com as mudanças de forma diferente do AWS Control Tower. AWS Service Catalog pode criar uma mudança na postura de governança quando ela reconcilia suas mudanças. Para obter mais informações sobre a atualização de um produto provisionado, consulte Atualização de produtos provisionados na documentação. AWS Service Catalog

## Referindo-se a recursos fora da AWS Control Tower

Quando você cria novas OUs e contas fora da AWS Control Tower, elas não são governadas pela AWS Control Tower, mesmo que possam ser exibidas.

Criar uma UO

As unidades organizacionais (OUs) criadas fora do AWS Control Tower são chamadas de não registradas. Eles são exibidos na página da organização, mas não são governados pelos controles do AWS Control Tower.

Criar uma conta

As contas criadas fora do AWS Control Tower são chamadas de não inscritas. As contas inscritas e não inscritas que pertencem a uma OU registrada no AWS Control Tower são exibidas na página da organização. Contas que não pertencem a uma OU registrada podem ser convidadas usando o AWS Organizations console. Esse convite para participar não inscreve a conta na AWS Control Tower nem estende a governança da AWS Control Tower à conta. Para ampliar a governança inscrevendo a conta, acesse a página da organização ou a página de detalhes da conta no AWS Control Tower e escolha Inscrever conta.

## Alteração externa dos nomes dos recursos do AWS Control Tower

Você pode alterar os nomes de suas unidades organizacionais (OUs) e contas fora do console do AWS Control Tower, e o console é atualizado automaticamente para refletir essas alterações.

Renomear uma UO

Em AWS Organizations, você pode alterar o nome de uma OU usando a AWS Organizations API ou o console. Quando você altera o nome de uma OU fora do AWS Control Tower, o console do

AWS Control Tower reflete automaticamente a alteração do nome. No entanto, se você provisionar suas contas usando AWS Service Catalog, você também deverá redefinir sua landing zone para garantir que o AWS Control Tower permaneça consistente com AWS Organizations. O fluxo de trabalho de redefinição garante a consistência entre os serviços das OUs básicas e adicionais. Você pode resolver esse tipo de desvio na página de configurações da zona de pouso. Consulte a seção chamada “Resolvendo o desvio” em. Detecte e resolva desvios na AWS Control Tower

O AWS Control Tower exibe os nomes das OUs na página da organização no painel da AWS Control Tower. Você pode ver quando sua operação de redefinição da zona de pouso foi bem-sucedida.

Renomear uma conta registrada

Cada AWS conta tem um nome de exibição que pode ser alterado pelo usuário raiz da conta no AWS Billing and Cost Management console. Quando você renomeia uma conta que está inscrita no AWS Control Tower, a mudança de nome é automaticamente refletida no AWS Control Tower. Para obter mais informações sobre como alterar o nome de uma conta, consulte Gerenciamento de uma AWS conta no Guia do usuário AWS de faturamento.

## Excluindo a OU de segurança

Esse tipo de oscilação é um caso especial. Se você excluir o Security OU, você verá uma página de mensagem de erro solicitando que você redefina sua landing zone. Você deve redefinir sua landing zone antes de realizar qualquer outra ação no AWS Control Tower.

- Você não poderá realizar nenhuma ação no console do AWS Control Tower e não poderá criar novas contas AWS Service Catalog até que a redefinição seja feita.
- Você não conseguirá visualizar a página de configurações da zona de pouso para ver o botão Redefinir lá.

Nessa situação, o processo de redefinição da landing zone cria uma nova OU de segurança e move as duas contas compartilhadas para a nova OU de segurança. O AWS Control Tower marca as contas de arquivamento de registros e auditoria como desviadas. O mesmo processo resolve o desvio nessas contas.

Se você determinar que deve excluir a OU de segurança, aqui está o que você precisa saber:

Antes de excluir a OU de segurança, você deve se certificar de que ela não contém contas. Especificamente, você deve remover as contas de Arquivo de Registros e Auditoria da OU. Recomendamos que você mova essas contas para outra UO.

> **Note**
>
> A ação de excluir sua OU de segurança não deve ser executada sem a devida consideração. A ação pode criar problemas de conformidade se o registro for suspenso temporariamente e porque alguns controles podem não ser aplicados.

Para obter informações gerais sobre oscilação, consulte "Resolver oscilações" em Detecte e resolva desvios na AWS Control Tower.

## Removendo uma conta da OU de segurança

Não recomendamos que você remova nenhuma das contas compartilhadas da sua organização nem as retire da OU de Segurança. Se você removeu uma conta compartilhada acidentalmente, siga as etapas de correção nesta seção para restaurar a conta.

- De dentro do console do AWS Control Tower: Para iniciar o processo de remediação, siga as etapas de remediação semimanuais. Certifique-se de que o usuário ou a função que você usa para acessar o console do AWS Control Tower tenha permissões para execução`organizations:InviteAccountToOrganization`. Se você não tiver essas permissões, siga as etapas de remediação manual, que usam tanto o console do AWS Control Tower quanto o AWS Organizations console.
- Começando pelo AWS Organizations console: esse processo de correção é um procedimento um pouco mais longo, totalmente manual. Ao seguir as etapas de remediação manual, você alternará entre o AWS Organizations console e o console do AWS Control Tower. Ao trabalhar em AWS Organizations, você precisará de um usuário ou função com a política `AWSOrganizationsFullAccess` gerenciada ou equivalente. Ao trabalhar no console da AWS Control Tower, você precisará de um usuário ou função com a política `AWSControlTowerServiceRolePolicy` gerenciada ou equivalente, além de permissão para executar todas as ações da AWS Control Tower (controltower: *).
- Se as etapas de correção não restaurarem a conta, entre em contato com AWS Support.

Os resultados da remoção de uma conta compartilhada por meio de AWS Organizations:

- A conta não está mais protegida pelos controles obrigatórios do AWS Control Tower com políticas de controle de serviços (SCPs). Resultado: os recursos criados pelo AWS Control Tower na conta podem ser modificados ou excluídos.

- A conta não está mais sob a conta AWS Organizations de gerenciamento. Resultado: o administrador da conta AWS Organizations de gerenciamento não tem mais visibilidade dos gastos da conta.
- Não é mais garantido que a conta seja monitorada por AWS Config. Resultado: o administrador da conta AWS Organizations de gerenciamento talvez não consiga detectar alterações nos recursos.
- A conta não está mais na organização. Resultado: as atualizações e redefinições do AWS Control Tower falharão.

Para restaurar uma conta compartilhada usando o console do AWS Control Tower (procedimento semimanal)

1. Faça login no console do AWS Control Tower em https://console.aws.amazon.com/controltower. Você deve fazer login como usuário do IAM, usuário no IAM Identity Center ou função com permissões para executar`organizations:InviteAccountToOrganization`. Se você não tiver essas permissões, use o procedimento de correção manual descrito posteriormente neste tópico.
2. Na página Detectada de desvio na zona de destino, escolha Convidar novamente para remediar a remoção da conta compartilhada, convidando novamente a conta compartilhada para a organização. Um e-mail gerado automaticamente é enviado para o endereço de e-mail da conta.
3. Aceite o convite para trazer a conta compartilhada de volta para a organização. Execute um destes procedimentos:
   - Faça login na conta compartilhada que foi removida e acesse https://console.aws.amazon.com/organizations/home#/invites
   - Se você tiver acesso à mensagem de e-mail enviada quando convidou novamente a conta, faça login na conta removida e clique no link na mensagem para navegar diretamente até o convite da conta.
   - Se a conta compartilhada que foi removida não estiver em outra organização, entre na conta, abra o AWS Organizations console e navegue até Convites.
4. Faça login na conta de gerenciamento novamente ou recarregue o console do AWS Control Tower se ele já estiver aberto. Você verá a página de deriva da zona de pouso. Escolha Redefinir para reparar a landing zone.
5. Aguarde a conclusão do processo de reinicialização.

Se a correção for bem-sucedida, a conta compartilhada aparecerá em um estado normal e em conformidade.

Se as etapas de correção não restaurarem a conta, entre em contato com AWS Support.

Para restaurar uma conta compartilhada usando o AWS Control Tower e AWS Organizations os consoles (remediação manual)

1. Faça login no AWS Organizations console emhttps://console.aws.amazon.com/organizations/. Você deve fazer login como usuário do IAM, usuário no IAM Identity Center ou função com a política `AWSOrganizationsFullAccess` gerenciada ou equivalente.
2. Convide a conta compartilhada de volta para a organização. Para obter informações sobre os requisitos, pré-requisitos e procedimentos para convidar uma conta AWS Organizations, consulte Convidar uma AWS conta para sua organização no Guia do usuário.AWS Organizations
3. Faça login na conta compartilhada que foi removida e acesse https://console.aws.amazon.com/organizations/home#/invites para aceitar o convite.
4. Faça login na conta de gerenciamento novamente.
5. Faça login no console da AWS Control Tower como usuário ou função com a política `AWSControlTowerServiceRolePolicy` gerenciada ou equivalente e permissões para executar todas as ações da AWS Control Tower (controltower: *).
6. Você verá a página de desvio da zona de pouso com a opção de redefinir a zona de pouso. Escolha Redefinir para reparar a landing zone.
7. Aguarde a conclusão do processo de reinicialização.

Se a correção for bem-sucedida, a conta compartilhada aparecerá em um estado normal e em conformidade.

Se as etapas de correção não restaurarem a conta, entre em contato com AWS Support.

## Alterações externas que são atualizadas automaticamente

As alterações que você faz nos endereços de e-mail da sua conta são atualizadas automaticamente pelo AWS Control Tower, mas o Account Factory não as atualiza automaticamente.

Alterar o endereço de e-mail de uma conta controlada

O AWS Control Tower recupera e exibe endereços de e-mail conforme exigido pela experiência do console. Portanto, os endereços de e-mail compartilhados e de outras contas são atualizados e exibidos de forma consistente no AWS Control Tower depois que você os altera.

> **Note**
>
> Em AWS Service Catalog, o Account Factory exibe os parâmetros que foram especificados no console quando você criou um produto provisionado. No entanto, o endereço de e-mail da conta original não será atualizado automaticamente quando o endereço de e-mail da conta for alterado. Isso ocorre porque a conta está contida conceitualmente no produto provisionado; não é a mesma que o produto provisionado. Para atualizar esse valor, é necessário atualizar o produto provisionado, o que pode causar uma alteração na postura de governança.

Aplicação de AWS Config regras externas

O AWS Control Tower exibe o status de conformidade de todas AWS Config as regras implantadas em unidades organizacionais registradas na AWS Control Tower, incluindo regras que foram ativadas fora do console do AWS Control Tower.

## Excluindo recursos da AWS Control Tower fora da AWS Control Tower

Você pode excluir OUs e contas no AWS Control Tower e não precisa realizar nenhuma ação adicional para ver as atualizações. O Account Factory é atualizado automaticamente quando você exclui uma OU, mas não quando você exclui uma conta.

Excluindo uma OU registrada (exceto a OU de segurança)

Dentro AWS Organizations, você pode remover unidades organizacionais (OUs) vazias usando a API ou o console. As UOs que contêm contas não podem ser excluídas.

O AWS Control Tower recebe uma notificação AWS Organizations quando uma OU é excluída. Ele atualiza a lista de UOs no Account Factory, para que a lista de OUs registradas permaneça consistente.

> **Note**
>
> Em AWS Service Catalog, o Account Factory é atualizado para remover a OU excluída da lista de OUs disponíveis nas quais você pode provisionar uma conta.

### Excluir uma conta registrada de uma UO

Quando você exclui uma conta cadastrada, o AWS Control Tower recebe uma notificação e faz atualizações para que as informações permaneçam consistentes.

> **Note**
>
> Em AWS Service Catalog, o produto provisionado pela Account Factory que representa a conta controlada não é atualizado para excluir a conta. Em vez disso, o produto provisionado é exibido como `TAINTED` e em um estado de erro. Para limpar, acesse o AWS Service Catalog, escolha o produto provisionado e escolha Terminate (Encerrar).

# Governe organizações e contas com a AWS Control Tower

Todas as unidades organizacionais (OUs) e contas que você cria na AWS Control Tower são governadas automaticamente pela AWS Control Tower. Além disso, se você tiver contas existentes OUs e que foram criadas fora da AWS Control Tower, você pode trazê-las para a governança da AWS Control Tower.

Para contas existentes AWS Organizations e AWS contas, a maioria dos clientes prefere inscrever grupos de contas registrando toda a unidade organizacional (OU) que contém as contas. Você também pode cadastrar contas individualmente. Para obter mais informações sobre a inscrição de contas individuais, consulteInscrever um existente Conta da AWS.

Terminologia

- Quando você traz uma organização existente para a AWS Control Tower, isso se chama registrar a organização ou estender a governança à organização.
- Quando você traz uma AWS conta para a AWS Control Tower, isso se chama cadastrar a conta.

Visualize suas contas OUs e

Na página AWS Control Tower Organization, você pode ver todas as suas AWS Organizations, incluindo OUs as registradas OUs na AWS Control Tower e as que não estão registradas. Você pode ver aninhado OUs como parte da hierarquia. Uma maneira fácil de visualizar suas unidades organizacionais na página Organização é selecionar somente unidades organizacionais no menu suspenso no canto superior direito.

A página Organização lista todas as contas em sua organização, independentemente da OU ou do status de inscrição na AWS Control Tower. Uma maneira fácil de visualizar suas contas na página Organização é selecionar Contas somente no menu suspenso no canto superior direito. Você pode visualizar, atualizar e inscrever contas individualmente noOUs, se as contas atenderem aos pré-requisitos de inscrição.

Se você não selecionar nenhum filtro, a página Organização exibirá suas contas e OUs em uma hierarquia. É um local central para monitorar e realizar ações em todos os recursos da AWS Control Tower. Para obter mais informações sobre a página da organização, você pode ver o vídeo passo a passo.

# Demonstração em vídeo

Este vídeo (4:01) descreve como trabalhar com a página Organização no AWS Control Tower. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Passo a passo em vídeo sobre como trabalhar com a página da organização no AWS Control Tower.

Tópicos

- Registre uma unidade organizacional existente na AWS Control Tower
- Inscrever um existente Conta da AWS

# Estenda a governança a uma organização existente

Você pode adicionar a governança da AWS Control Tower a uma organização existente configurando uma landing zone (LZ) conforme descrito no Guia do usuário da AWS Control Tower em Getting Started, Etapa 2.

Veja o que esperar ao configurar sua landing zone da AWS Control Tower em uma organização existente.

- Você pode ter uma landing zone por AWS Organizations organização.
- AWSA Control Tower usa a conta de gerenciamento da sua AWS Organizations organização existente como sua conta de gerenciamento. Nenhuma nova conta de gerenciamento é necessária.
- AWSA Control Tower configura duas novas contas em uma OU registrada: uma conta de auditoria e uma conta de registro.
- Os limites de serviço da sua organização devem permitir a criação dessas duas contas adicionais.
- Depois de lançar sua landing zone ou registrar uma OU, os controles da AWS Control Tower se aplicam automaticamente a todas as contas inscritas nessa OU.
- Você pode inscrever outras AWS contas existentes em uma OU que seja governada pela AWS Control Tower, para que os controles se apliquem a essas contas.
- Você pode adicionar mais OUs na AWS Control Tower e registrar os existentesOUs.

Para verificar outros pré-requisitos para registro e inscrição, consulte Getting Started with Control Tower. AWS

Aqui estão mais detalhes sobre como os controles da AWS Control Tower não se aplicam às suas OUs AWS organizações que não têm zonas de pouso da AWS Control Tower configuradas:

- Novas contas criadas fora do AWS Control Tower Account Factory não estão vinculadas aos controles da OU registrada.
- Novas contas criadas OUs que não estão registradas na AWS Control Tower não estão vinculadas a controles, a menos que você inscreva especificamente essas contas na AWS Control Tower. Consulte Inscrever um existente Conta da AWS para obter mais informações sobre como registrar contas.
- Outras organizações existentes, contas existentes e quaisquer contas novas OUs ou criadas por você fora da AWS Control Tower não estão vinculadas aos controles da AWS Control Tower, a menos que você registre separadamente a OU registre a conta.

Para obter mais informações sobre como aplicar o AWS Control Tower às contas existentes OUs e às contas, consulteRegistre uma unidade organizacional existente na AWS Control Tower.

Para uma visão geral do processo de configuração de uma landing zone da AWS Control Tower em sua organização existente, veja o vídeo na próxima seção.

> **Note**
>
> Durante a configuração, a AWS Control Tower realiza pré-verificações para evitar problemas comuns. No entanto, se você estiver usando atualmente a solução AWS Landing Zone para AWS Organizations, consulte seu arquiteto de AWS soluções antes de tentar habilitar a AWS Control Tower em sua organização para determinar se a AWS Control Tower pode interferir na implantação atual da sua zona de pouso. Além disso, consulte Se a conta não atender aos pré-requisitos para obter informações sobre como mover contas de um landing zone para outro.

## Vídeo: Ativar uma zona de aterrissagem existente AWS Organizations

Este vídeo (7:48) descreve como configurar e habilitar uma zona de pouso da AWS Control Tower em AWS Organizations estruturas existentes. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Habilite o AWS Control Tower para organizações existentes

## Considerações para o IAM Identity Center e organizações existentes

- Se o AWS IAM Identity Center (IAMIdentity Center) já estiver configurado, a região de origem do AWS Control Tower deverá ser a mesma que a região do IAM Identity Center.
- AWSO Control Tower não exclui uma configuração existente.
- Se o IAM Identity Center já estiver ativado e você estiver usando o IAM Identity Center Directory, o AWS Control Tower adicionará recursos como conjuntos de permissões, grupos e assim por diante, e prosseguirá normalmente.
- Se outro diretório (externo, AD, AD gerenciado) estiver configurado, o AWS Control Tower não alterará a configuração existente. Para obter mais detalhes, consulte Considerações para clientes AWS IAM Identity Center (IAM Identity Center).

## Acesso a outros AWS serviços

Depois de incorporar sua organização à governança da AWS Control Tower, você ainda terá acesso a todos os AWS serviços disponíveis por meio do AWS Organizations console APIs e. AWS Organizations Para obter mais informações, consulte Serviços relacionados da AWS.

# OUs aninhadas na AWS Control Tower

Este capítulo lista as expectativas e considerações que você deve conhecer ao trabalhar com OUs aninhadas no AWS Control Tower. Na maioria das formas, trabalhar com OUs aninhadas é o mesmo que trabalhar com uma estrutura de OU plana. Os recursos de Registro e Registro Novo funcionam com OUs aninhadas, exceto pelos comportamentos alterados que são observados neste capítulo.

## Passo a passo em vídeo

Este vídeo (4:46) descreve como gerenciar implantações de OU aninhadas no AWS Control Tower. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Vídeo passo a passo do gerenciamento de OUs aninhadas no AWS Control Tower.

Para obter orientação sobre as melhores práticas para OUs aninhadas e sua zona de pouso, consulte a postagem do blog Organizando sua zona de pouso do AWS Control Tower com OUs aninhadas.

# Expandir de uma estrutura de OU plana para uma estrutura de OU aninhada

Se você criou sua landing zone do AWS Control Tower com uma estrutura de OU plana, você pode expandi-la para uma estrutura de OU aninhada.

Esse processo tem quatro etapas principais:

1. Crie sua estrutura de OU aninhada desejada no AWS Control Tower.
2. Acesse o AWS Organizations console e use o recurso de movimentação em massa para mover as contas da OU de origem (plana) para a OU de destino (aninhada). Veja como:
   a. Vá para a OU da qual você deseja mover contas.
   b. Selecione todas as contas na OU.
   c. Selecione Mover.

   > **Note**
   >
   > Essa etapa deve ser realizada no AWS Organizations console interno porque o AWS Control Tower não tem o recurso Move.

3. Acesse a OU aninhada no AWS Control Tower e registre-a ou registre-a novamente. Todas as contas na OU aninhada serão inscritas.
   - Se você criou a OU no AWS Control Tower, registre novamente a OU.
   - Se você criou a OU em AWS Organizations, registre a OU pela primeira vez.
4. Depois que suas contas forem movidas e registradas, exclua a OU vazia de nível superior, do AWS Organizations console ou do console do AWS Control Tower.

## Pré-verificações de registro de OU aninhadas

Para apoiar o registro bem-sucedido de suas OUs aninhadas e de suas contas de membros, o AWS Control Tower realiza uma série de pré-verificações. Essas mesmas verificações prévias são realizadas ao registrar qualquer UO de nível superior ou UO aninhada. Para obter mais informações, consulte Causas comuns de falha durante o registro ou o novo registro.

- Se todas as pré-verificações forem aprovadas, o AWS Control Tower começará a registrar sua OU automaticamente.

- Se alguma pré-verificação falhar, o AWS Control Tower interrompe o processo de registro e fornece uma lista de itens que devem ser corrigidos antes que você possa registrar sua OU.

## OUs e funções aninhadas

O AWS Control Tower implanta a `AWSControlTowerExecution` função em contas na OU de destino e em contas em todas as OUs aninhadas na OU de destino, mesmo quando sua intenção é registrar somente a OU de destino. Essa função concede a qualquer usuário da conta de gerenciamento permissões de administrador em qualquer conta que tenha a `AWSControlTowerExecution` função. A função pode ser usada para realizar ações que normalmente não seriam permitidas pelos controles do AWS Control Tower.

Você pode excluir essa função de contas não inscritas que você não planeja inscrever. Se você excluir essa função, não poderá registrar a conta no AWS Control Tower nem registrar as OUs principais imediatas, a menos que você restaure a função na conta. Para excluir a `AWSControlTowerExecution` função de uma conta, você deve estar conectado com a `AWSControlTowerExecution` função, porque nenhum outro diretor do IAM tem permissão para excluir funções gerenciadas pelo AWS Control Tower.

Para obter informações sobre como restringir o acesso à função, consulte Condições opcionais para as relações de confiança da sua função.

## O que acontece durante o registro e o novo registro de OUs e contas aninhadas

Quando você registra ou registra novamente uma OU aninhada, o AWS Control Tower inscreve todas as contas não inscritas da OU de destino e atualiza todas as contas inscritas. Aqui está o que esperar.

O AWS Control Tower executa as seguintes tarefas

- Adiciona a `AWSControlTowerExecution` função a todas as contas não inscritas nesta OU e a todas as contas não inscritas em suas OUs aninhadas.
- Registra contas de membros que não estão inscritas.
- Reinscreve as contas dos membros inscritos.
- Cria um login do IAM Identity Center para contas de membros recém-inscritas.
- Atualiza as contas de membros inscritos existentes para refletir as mudanças na sua landing zone.

- Atualiza os controles que estão configurados para essa OU e suas contas de membros.

## Considerações sobre o registro de OU aninhada

- Você não pode registrar uma OU na OU principal (OU de segurança).
- As OUs aninhadas devem ser registradas separadamente.
- Você não pode registrar uma OU a menos que sua OU principal esteja registrada.
- Você não pode registrar uma OU a menos que todas as OUs superiores na árvore tenham sido registradas com sucesso em algum momento (algumas podem ter sido excluídas).
- Você pode registrar uma OU que esteja sob uma OU derivada superior, mas a variação não é reparada por essa ação.

## Limitações de UO aninhadas

- As OUs podem estar aninhadas a no máximo 5 níveis de profundidade abaixo da raiz.
- As OUs aninhadas na OU de destino devem ser registradas ou registradas novamente separadamente.
- Se a OU de destino estiver no nível 2 ou abaixo na hierarquia, ou seja, se não for uma OU de nível superior, os controles preventivos habilitados em OUs superiores serão aplicados automaticamente nessa OU e em todas as OUs abaixo dela.
- As falhas de registro da OU não se propagam na árvore hierárquica. Você pode ver detalhes sobre os estados das OUs aninhadas na página de detalhes da OU dos pais.
- As falhas de registro da OU não se propagam pela árvore hierárquica.
- O AWS Control Tower não modifica suas configurações de VPC para nenhuma conta nova ou existente.

## OUs aninhadas e conformidade

No console do AWS Control Tower, você pode visualizar OUs e contas que não estão em conformidade na página da organização, para que você possa entender a conformidade em uma escala maior.

Considerações sobre conformidade para OUs e contas aninhadas

- A conformidade de uma OU não é determinada com base na conformidade das OUs aninhadas nela.
- O status de conformidade de um controle é calculado em todas as OUs nas quais o controle está ativado, incluindo OUs aninhadas. Veja o status de conformidade do AWS Control Tower para UOs e contas w.
- Uma OU é mostrada como não compatível somente se tiver contas incompatíveis, independentemente de onde a OU esteja na hierarquia da OU.
- Se uma OU aninhada não estiver em conformidade, sua OU principal não será automaticamente considerada incompatível.
- Na página de detalhes da OU ou na página de detalhes da conta, você pode ver uma lista de recursos não compatíveis que podem estar fazendo com que suas OUs ou contas mostrem um status de não conformidade.

## UOs aninhadas e drift

Em determinadas situações, o desvio pode impedir o registro de OUs aninhadas.

Expectativas de OUs flutuantes e aninhadas

- Você pode ativar controles em OUs com pais desviados, mas não diretamente em OUs desviados.
- Você tem permissão para ativar os controles de detetive em uma OU desviada, desde que não seja uma OU desviada de nível superior.
- Os controles obrigatórios são habilitados somente em OUs de nível superior. Os controles obrigatórios são ignorados quando você registra uma OU aninhada.
- Um controle obrigatório protege AWS Config os recursos; portanto, esse controle deve estar em um estado não desviado para registrar OUs aninhadas. Se for desviado, o AWS Control Tower bloqueia o registro de OUs aninhadas.
- Se a OU de nível superior estiver em desvio, o controle que protege os AWS Config recursos pode estar em desvio. Nessa situação, o AWS Control Tower bloqueia qualquer ação que exija a criação ou atualização de AWS Config recursos, incluindo a aplicação de controles de detetive.

# UOs e controles aninhados

Quando você ativa um controle em uma OU registrada, os controles preventivos e de detetive têm comportamentos diferentes. Para OUs aninhadas, os controles proativos se comportam de forma semelhante aos controles de detetive.

Controles preventivos

- Os controles preventivos são aplicados em OUs aninhadas.
- Os controles preventivos obrigatórios são aplicados em todas as contas da OU e de suas OUs aninhadas.
- Os controles preventivos afetam todas as contas e OUs aninhadas na OU de destino, mesmo que essas contas e OUs não estejam registradas.

Controles detectivos e proativos

- As OUs aninhadas não herdam controles de detetive ou proativos automaticamente; eles devem ser ativados separadamente.
- Controles detectivos e proativos são implantados somente em contas registradas nas regiões operacionais da sua zona de pouso.

Estados de controle e herança habilitados

Você pode ver os controles herdados de cada UO na página de detalhes da UO.

> **Tip**
>
> Você pode usar a herança de controle para ajudar a permanecer dentro da cota de SCP de uma OU. Por exemplo, você pode habilitar um controle na OU de nível superior de uma hierarquia de OU, em vez de habilitar diretamente para uma OU aninhada.

Status herdado

- O status Herdado indica que o controle é ativado somente por herança e não foi aplicado diretamente à OU.
- O status Ativado significa que o controle é aplicado nessa OU, independentemente de seu estado em outras OUs.

- O status Falha significa que o controle não é aplicado nesta OU, independentemente de seu estado em outras OUs.

> **Note**
>
> O status Herdado indica que o controle foi aplicado a uma OU mais alta na árvore e é aplicado a essa OU, mas não foi adicionado diretamente a essa OU.

> **Se sua landing zone não for a versão atual**
>
> Cada linha na tabela de controles ativados representa um controle ativado em uma OU individual.

### UOs aninhadas e a raiz

A raiz não é uma UO e não pode ser registrada ou registrada novamente. Você também não pode criar contas diretamente na raiz. A raiz não pode ser incompatível nem ter um estado de ciclo de vida, como registrado ou em desvio.

No entanto, a raiz é o contêiner de nível superior para todas as contas e OUs. No contexto de OUs aninhadas, é o nó sob o qual todas as outras OUs estão aninhadas.

## Registre uma unidade organizacional existente na AWS Control Tower

Uma forma eficiente de incluir várias AWS contas existentes na AWS Control Tower é estender a governança da AWS Control Tower a toda uma unidade organizacional (OU).

Para habilitar a governança da AWS Control Tower sobre uma OU existente que foi criada com AWS Organizations, e suas contas, registre a OU em sua landing zone da AWS Control Tower. Você pode se registrar OUs que contenha até 1000 contas. Se uma OU contiver mais de 1000 contas, você não poderá registrá-la no AWS Control Tower.

Quando você registra uma OU, suas contas de membros são inscritas na landing zone da AWS Control Tower. Eles são governados pelos controles que se aplicam à sua OU.

> **Note**
>
> Se você ainda não tem uma zona de pouso da AWS Control Tower, comece configurando uma zona de pouso, seja em uma nova organização criada pela AWS Control Tower ou em uma AWS Organizations organização existente. Para obter mais detalhes sobre como configurar uma landing zone, consulteComece a usar o AWS Control Tower.

O que acontece com minhas contas quando eu registro minha OU?

AWSA Control Tower exige permissão para estabelecer acesso confiável entre AWS CloudFormation e AWS Organizations em seu nome, para que AWS CloudFormation possa implantar sua pilha nas contas da sua organização automaticamente.

- A `AWSControlTowerExecution` função é adicionada a todas as contas com o status Não inscrito.
- Os controles obrigatórios são habilitados por padrão para sua OU e todas as suas contas quando você registra sua OU.

Inscrição parcial de contas após o registro de uma OU

É possível registrar uma OU com sucesso, mas algumas contas podem permanecer não registradas. Nesse caso, essas contas não atendem a alguns dos pré-requisitos para inscrição. Se a inscrição de uma conta como parte do processo de Registrar OU não for bem-sucedida, o status da conta na página de contas mostrará Falha na inscrição. Você também pode ver as informações da conta na sua página de OU, como 4 de 5, no campo contas.

Por exemplo, se você ver 4 de 5, isso significa que sua OU tem 5 contas no total, e 4 delas foram inscritas com sucesso, mas uma conta falhou ao se inscrever durante o processo de Registro de OU. Você pode escolher Registrar novamente a OU para inscrever as contas, depois de verificar se as contas atendem aos pré-requisitos de inscrição.

IAMpré-requisitos do usuário para registrar uma OU

Sua identidade AWS Identity and Access Management (IAM) (usuário ou função) ou IAM identidade de usuário do Identity Center deve ser incluída no portfólio apropriado do Account Factory quando você executa a operação Register OU, mesmo que você já tenha `Admin` permissões. Caso contrário, a criação dos produtos provisionados falhará durante o registro. A falha ocorre porque o AWS

Control Tower depende das credenciais do IAM usuário ou da IAM identidade do usuário do Identity Center ao registrar uma OU.

O portfólio relevante é aquele criado pela AWS Control Tower, chamado AWSControl Tower Account Factory Portfolio. Navegue até ele escolhendo Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio. Em seguida, selecione a guia chamada Grupos, funções e usuários para visualizar sua IAM identidade IAM ou a do Identity Center. Para obter mais informações sobre como conceder acesso, consulte a documentação do AWS Service Catalog.

## Registrar uma OU existente

No console da AWS Control Tower, na página Organização, você pode visualizar todas as contas OUs e organizações em uma hierarquia, incluindo OUs aquelas registradas na AWS Control Tower e aquelas que não estão registradas.

Em geral, os não registrados OUs foram criados em AWS Organizations, e não são governados por nenhuma outra landing zone. Você pode registrar contas existentes OUs que contenham até 1000 contas. Se uma OU contiver mais de 1000 contas, você não poderá registrá-la no AWS Control Tower.

Para registrar uma OU existente

1. Faça login no console da AWS Control Tower em https://console.aws.amazon.com/controltower.
2. No menu de navegação do painel esquerdo, escolha Organização.
3. Na página Organização, selecione o botão de rádio ao lado da OU que você deseja registrar e, em seguida, selecione Registrar unidade organizacional no menu suspenso Ações no canto superior direito ou, alternativamente, selecione o nome da OU para que você possa visualizar a página de detalhes da OU dessa OU.
4. Na página de detalhes da OU, no canto superior direito, você pode selecionar Registrar OU no menu suspenso Ações.

O processo de registro leva no mínimo 10 minutos para estender a governança à OU e até 2 minutos adicionais para cada conta adicional.

Resultados do registro de uma OU existente

Depois de registrar uma OU existente, a `AWSControlTowerExecution` função permite que a AWS Control Tower estenda a governança às suas contas individuais. As grades de proteção são

aplicadas e as informações sobre as atividades da conta são reportadas às suas contas de auditoria e registro.

Outros resultados incluem o seguinte:

- `AWSControlTowerExecution`permite a auditoria pela conta de auditoria da AWS Control Tower.
- `AWSControlTowerExecution`ajuda você a configurar o registro de sua organização, para que todos os registros de cada conta sejam enviados para a conta de registro.
- `AWSControlTowerExecution`garante que os controles selecionados da AWS Control Tower se apliquem automaticamente a cada conta individual em sua contaOUs, bem como a cada nova conta que você criar na AWS Control Tower.

Para uma OU registrada, você pode fornecer relatórios de conformidade e segurança com base nos recursos de auditoria e registro incorporados pelos AWS controles da Control Tower. Suas equipes de segurança e conformidade podem verificar se todos os requisitos foram atendidos e se houve algum desvio organizacional. Para obter mais informações sobre deriva, consulteDetecte e resolva desvios na AWS Control Tower.

> **Note**
>
> Uma situação incomum pode ocorrer quando a AWS Control Tower OUs e suas contas são exibidas. Se você criou uma conta em uma OU registrada e, posteriormente, transferiu essa conta inscrita para outra OU que não está registrada, especialmente se você usa AWS Organizations para mover a conta, você pode ver o resultado “1 de 0” contas na página de detalhes da OU. Além disso, você pode ter criado outra conta não registrada nessa OU não registrada. Se houver uma conta não registrada, o console poderá ler “1 de 1” para a OU. Parece que a conta única (recém-criada) está inscrita, mas na verdade não está. Você deve cadastrar a nova conta.

## Crie uma nova OU

Veja como criar uma OU ou uma OU aninhada na AWS Control Tower.

Para criar uma nova OU na AWS Control Tower

1. Navegue até a página Organização.

2. Selecione Criar unidade organizacional no menu suspenso Criar recursos no canto superior direito.
3. Especifique um nome no campo Nome da OU.
4. No menu suspenso OU principal, você pode ver a hierarquia dos registrados. OUs Selecione uma OU principal para a nova OU que você está criando.
5. Escolha Adicionar.

> **Tip**
>
> Para adicionar uma OU aninhada em menos etapas, selecione o nome da OU principal mostrado na tabela na página Organização, visualize a página de OU dessa OU principal e escolha Adicionar uma OU no menu suspenso Ações no canto superior direito. A nova OU é criada automaticamente como uma OU aninhada na OU selecionada.

> **Note**
>
> Se sua landing zone não estiver atualizada, você verá uma lista plana em vez de uma hierarquia no menu suspenso. Mesmo que sua landing zone inclua unidades aninhadasOUs, você não verá UOs de nível 5 no menu suspenso, pois não é possível criar uma nova unidade organizacional abaixo de uma unidade organizacional de nível 5. Para obter mais informações sobre aninhado OUs na AWS Control Tower, consulteOUs aninhadas na AWS Control Tower.

## Causas comuns de falha durante o registro ou o novo registro

Em geral, quando você registra ou registra novamente uma OU, todas as contas dentro dessa OU são inscritas na AWS Control Tower. No entanto, é possível que algumas contas não consigam se inscrever, mesmo que a OU como um todo seja registrada com sucesso. Nesses casos, você deve resolver a falha de pré-verificação relacionada à conta e, em seguida, tentar reinscrever essa conta ou OU.

Se o registro (ou o novo registro) de uma OU ou de qualquer uma de suas contas membros falhar, o AWS Control Tower retornará mensagens de erro para as contas de membros afetadas. Você pode visualizar as mensagens de erro na página de detalhes da OU, na qual uma tabela agrega as pré-

verificações e as mensagens de erro da conta. Se uma operação de Registrar OU falhar, a tabela mostrará todas as mensagens de erro de todas as contas na OU. Se necessário, você também pode ver as mensagens de erro na página de detalhes da conta de cada conta.

Opcionalmente, você pode baixar um arquivo contendo um relatório detalhado que mostra quais pré-verificações não foram aprovadas, para análise off-line. Você pode concluir o download escolhendo o botão Download, que aparece no canto superior direito da área de registro.

Esta seção lista os tipos de erros que você pode receber se as pré-verificações falharem e como corrigi-los.

Erro na zona de pouso

- A zona de pouso não está pronta

  Redefina sua landing zone atual ou atualize-a para a versão mais recente.

Erros de OU

- Excede o número máximo de SCPs

  Você pode estar acima do limite de políticas de controle de serviço (SCPs) por UO ou pode ter atingido outra cota. Um limite de 5 SCPs por UO se aplica a todos OUs na sua landing zone da AWS Control Tower. Se você tiver SCPs mais do que o permitido pela cota, deverá excluir ou combinar o. SCPs
- Conflitante SCPs

  O existente SCPs pode ser aplicado à OU ou à conta, o que impede que a AWS Control Tower registre a conta. Verifique se a política aplicada SCPs pode impedir que a AWS Control Tower funcione. Certifique-se de verificar os SCPs que são herdados de uma posição OUs superior na hierarquia.
- Excede a cota do conjunto de pilhas

  A cota do conjunto de pilhas pode ter sido excedida. Se você tiver mais instâncias do que a cota permite, exclua algumas instâncias de pilha. Para obter mais informações, consulte Cotas do AWS CloudFormation no Guia do usuário do AWS CloudFormation .
- Excede o limite da conta

  AWSA Control Tower limita cada OU a 1000 contas durante o registro.

Erros na conta

- Verificações prévias evitadas em contas

  Uma existência SCP na OU impede que a AWS Control Tower realize verificações prévias em suas contas de membros da OU. Para resolver essa falha de pré-verificação, atualize ou remova o SCP da OU.

- Erro de endereço de e-mail

  O endereço de e-mail que você especificou para a conta não está em conformidade com os padrões de nomenclatura. Aqui está a expressão regular (regex) que especifica quais caracteres são permitidos: `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Config gravador ou canal de entrega ativado

  A conta pode ter um gravador AWS Config de configuração ou canal de entrega existente. Eles devem ser excluídos ou modificados AWS CLI em todas as AWS regiões em que a conta de gerenciamento da AWS Control Tower tenha recursos controlados, antes que você possa inscrever uma conta.

- STSdeficiente

  AWS Security Token Service (AWS STS) pode estar desativado na conta. AWS STSos endpoints devem ser ativados nas contas de todas as regiões suportadas pela AWS Control Tower.

- IAMConflito no Identity Center

  A região de origem da AWS Control Tower não é a mesma que a região AWS IAM Identity Center (Centro de IAM Identidade). Se o IAM Identity Center já estiver configurado, a região inicial do AWS Control Tower deverá ser a mesma da Região do IAM Identity Center.

- Tópico conflitante SNS

  A conta tem um nome de tópico do Amazon Simple Notification Service (AmazonSNS) que o AWS Control Tower precisa usar. AWSA Control Tower cria recursos (como SNS tópicos) com nomes específicos. Se esses nomes já tiverem sido usados, a configuração do AWS Control Tower falhará. Essa situação pode ocorrer se você estiver reutilizando uma conta anteriormente inscrita no AWS Control Tower.

- Conta suspensa detectada

  Essa conta foi suspensa. Ele não pode ser inscrito no AWS Control Tower. Remova a conta dessa OU e tente novamente.

- IAMusuário que não está no portfólio

  Adicione o usuário AWS Identity and Access Management (IAM) ao portfólio do Service Catalog antes de registrar sua OU. Esse erro se refere somente à conta de gerenciamento.

- A conta não atende aos pré-requisitos

  A conta não atende aos pré-requisitos para inscrição na conta. Por exemplo, a conta pode não ter as funções e as permissões necessárias para registrá-la na AWS Control Tower. As instruções para adicionar uma função estão disponíveis emAdicione manualmente a IAM função necessária a uma existente Conta da AWS e inscreva-a.

Como lembrete, AWS CloudTrail é ativado automaticamente em todas as suas AWS contas quando você as inscreve no Control TowerAWS. Se CloudTrail estiver ativado em uma conta antes da inscrição, você poderá experimentar o faturamento duplo, a menos que desative CloudTrail antes de iniciar o processo de inscrição.

# Atualizar organizações

A maneira mais rápida de atualizar uma unidade organizacional (OU) ou atualizar várias contas em uma OU é registrar novamente a OU.

## Quando atualizar a AWS Control Tower OUs e as contas

Ao realizar uma atualização da landing zone, você deve atualizar suas contas inscritas para aplicar novos controles a essas contas.

- Você pode realizar uma atualização em todas as contas em uma OU usando a opção Registrar novamente.
- Se você tiver mais de uma OU registrada em seu landing zone, registre novamente todas as suas OUs para atualizar todas as suas contas.
- Para atualizar uma única conta, você pode atualizar a partir do console AWS Control Tower ou selecionar a opção Atualizar produto provisionado em. AWS Service Catalog Consulte Atualize a conta no console.

## Atualizar várias contas na mesma OU

Repita essas etapas para cada OU em sua organização da AWS Control Tower, se precisar atualizar todas as suas contas OUs e.

Para atualizar várias contas em uma OU, com uma ação

1. Faça login no console da AWS Control Tower em https://console.aws.amazon.com/controltower.
2. No menu de navegação do painel esquerdo, escolha Organização.
3. Na página Organização, escolha qualquer OU para ver a página de detalhes da OU.
4. Em Ações no canto superior direito, selecione Registrar UO novamente.

Como alternativa, você pode selecionar qualquer conta que mostre o status Atualização disponível e, em seguida, escolher Atualizar conta, para quantas contas forem necessárias.

## O que acontece durante o novo registro

Quando você registra novamente uma OU:

- O campo Estado indica se a conta está atualmente inscrita no AWS Control Tower (Inscrita), se a conta nunca foi inscrita (Não inscrita) ou se a inscrição falhou anteriormente (Falha na inscrição).
- Quando você registra novamente a OU, a `AWSControlTowerExecution` função é adicionada a todas as contas com o status Não inscrito ou Falha na inscrição.
- AWSO Control Tower cria um login único (IAMIdentity Center) para essas novas contas inscritas.
- As contas inscritas são reinscritas no Control TowerAWS.
- O desvio em qualquer controle preventivo aplicado à OU é fixo, pois SCPs eles retornam às suas definições padrão.
- Todas as contas são atualizadas para refletir as mudanças mais recentes na landing zone.

Para obter mais informações, consulte Inscrever um existente Conta da AWS.

> **Tip**
>
> Ao registrar novamente uma OU ou ao atualizar sua versão do landing zone e várias contas de membros, você pode ver uma mensagem de falha mencionando o StackSet -. AWSControlTowerExecutionRole Isso StackSet na conta de gerenciamento pode falhar

porque a AWSControlTowerExecutionIAMfunção já existe em todas as contas de membros inscritos. Essa mensagem de erro é um comportamento esperado e pode ser ignorada.

## Atualizar uma única conta

Você pode atualizar contas individuais da AWS Control Tower no console da AWS Control Tower ou no console do Service Catalog.

Para atualizar uma única conta no console AWS Control Tower, consulteAtualize a conta no console.

Para atualizar uma única conta no AWS Service Catalog

1. Acesse AWS Service Catalog.
2. No menu de navegação do painel esquerdo, escolha Produtos provisionados.
3. Na página Produtos provisionados, selecione o botão de rádio ao lado do produto provisionado que você deseja atualizar.
4. No canto superior direito, escolha o menu suspenso Ações para Atualizar.

Para saber mais sobre a atualização em AWS Service Catalog, consulte Atualize o produto provisionado e atualizando produtos no Service Catalog Administrator Guide.

# Serviços integrados

O AWS Control Tower é um serviço criado com base em outros AWS serviços para ajudar você a configurar um ambiente bem arquitetado. Este capítulo fornece uma breve visão geral desses serviços, incluindo informações de configuração sobre os serviços subjacentes e como eles funcionam no AWS Control Tower.

Para obter mais informações sobre como medir um ambiente bem arquitetado, conheça a Well-Architected Tool AWS . Consulte também o Guia do ambiente de nuvem de gerenciamento e governança.

Tópicos

- Implemente ambientes com AWS CloudFormation
- Monitore eventos com CloudTrail
- Monitore recursos e serviços com CloudWatch
- Controle as configurações de recursos com AWS Config
- Gerencie permissões para entidades com o IAM
- AWS Key Management Service
- Execute funções de computação sem servidor com o Lambda
- Gerencie contas por meio de AWS Organizations
- Armazene objetos com o Amazon S3
- Monitore seu ambiente com o Security Hub
- Provisione contas por meio de AWS Service Catalog
- Rastreie alertas por meio do Amazon Simple Notification Service
- Crie aplicativos distribuídos com AWS Step Functions

## Implemente ambientes com AWS CloudFormation

AWS CloudFormation permite que você crie e provisione implantações de AWS infraestrutura de forma previsível e repetida. Ele ajuda você a aproveitar AWS os produtos para criar aplicativos altamente confiáveis, escaláveis e econômicos na nuvem, sem se preocupar em criar e configurar a infraestrutura subjacente. AWS AWS CloudFormation permite que você use um arquivo de modelo

para criar e excluir uma coleção de recursos juntos como uma única unidade (uma pilha). Para obter mais informações, consulte o Guia do usuário do AWS CloudFormation.

O AWS Control Tower usa AWS CloudFormation conjuntos de pilhas para aplicar controles nas contas. Para obter mais informações sobre como o AWS Control Tower AWS CloudFormation e o AWS funcionam juntos, consulte Crie AWS Control Tower recursos com AWS CloudFormation.

## Monitore eventos com CloudTrail

O AWS Control Tower é configurado AWS CloudTrail para permitir o registro e a auditoria centralizados. Com CloudTrail, a conta de gerenciamento pode analisar as ações administrativas e os eventos do ciclo de vida das contas dos membros.

CloudTrail ajuda você a monitorar seu AWS ambiente na nuvem mantendo um histórico de chamadas de AWS API para suas contas. Por exemplo, você pode identificar os usuários e as contas que chamaram as AWS APIs para serviços compatíveis CloudTrail, o endereço IP de origem a partir do qual as chamadas foram feitas e a hora em que as chamadas ocorreram. Você pode se CloudTrail integrar aos aplicativos usando a API, automatizar a criação de trilhas para sua organização, verificar o status de suas trilhas e controlar como os administradores ativam e desativam o CloudTrail login. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

## Monitore recursos e serviços com CloudWatch

CloudWatch A Amazon fornece uma solução de monitoramento confiável, escalável e flexível que você pode começar a usar em minutos. Não é mais necessário configurar, gerenciar e dimensionar sua própria infraestrutura e sistemas de monitoramento. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Para obter mais informações sobre como a Amazon CloudWatch trabalha com o AWS Control Tower, consulte Monitoramento.

## Controle as configurações de recursos com AWS Config

AWS Config fornece uma visão detalhada dos recursos associados à sua AWS conta, incluindo como eles são configurados, como estão relacionados entre si e como as configurações e seus relacionamentos mudaram ao longo do tempo. Para obter mais informações, consulte o Guia do desenvolvedor do AWS Config.

AWS Config os recursos provisionados pelo AWS Control Tower são marcados automaticamente com `aws-control-tower` um valor de. `managed-by-control-tower`

Para obter mais informações sobre como AWS Config monitora e registra recursos no AWS Control Tower e como ela cobra por eles, consulteMonitore as mudanças de recursos com AWS Config.

O AWS Control Tower usa Regras do AWS Config para implementar controles de detetive. Para obter mais informações, consulte Sobre os controles no AWS Control Tower.

## Gerencie permissões para entidades com o IAM

AWS Identity and Access Management (IAM) é um AWS serviço para controlar o acesso a outros AWS serviços. Com o IAM, você pode gerenciar centralmente usuários e credenciais de segurança, como chaves de acesso e permissões, que designam os AWS recursos aos quais seus usuários e aplicativos recebem acesso.

Quando você configura sua landing zone, vários grupos podem ser criados AWS IAM Identity Center automaticamente, se você selecionar o IAM como seu provedor de identidade. Esses grupos têm conjuntos de permissões que são políticas de permissões predefinidas do IAM. Seus usuários finais também podem usar o IAM para definir o escopo das permissões para usuários do IAM e outras entidades nas contas dos membros.

AWS Identity and Access Management (IAM) simplifica a forma como você gerencia o acesso a AWS contas e aplicativos de negócios. Você pode controlar o acesso e as permissões de usuário do IAM Identity Center em todas as suas AWS contas no AWS Control Tower.

Para obter mais informações, consulte o Guia do usuário do AWS IAM Identity Center.

Se você estiver baseado em um Região da AWS que não oferece suporte ao IAM, você pode trazer outro provedor de identidade para configurar e manter seus próprios usuários e grupos manualmente.

## AWS Key Management Service

AWS Key Management Service (AWS KMS) permite criar e controlar chaves que protegem seus dados. Opcionalmente, o AWS Control Tower permite que você criptografe seus dados com AWS KMS chaves de criptografia. Para obter informações sobre AWS KMS, consulte o Guia do desenvolvedor do AWS KMS.

Para obter informações sobre como configurar AWS KMS chaves com o AWS Control Tower, consulte Configurar AWS KMS chaves opcionalmente.

## Execute funções de computação sem servidor com o Lambda

Com AWS Lambda, você pode executar código sem provisionar ou gerenciar servidores. Você pode executar código para vários tipos de aplicativos ou serviços de back-end, sem a necessidade de sobrecarga administrativa adicional. Quando você carrega seu código, o Lambda pode executar e escalar o código com alta disponibilidade. Você pode configurar seu código para ser acionado automaticamente a partir de outros AWS serviços ou pode chamá-lo diretamente de qualquer aplicativo móvel ou da web.

Por exemplo, determinadas funções na conta de auditoria do AWS Control Tower podem ser assumidas programaticamente, para que você possa revisar outras contas usando o Lambda. Além disso, você pode usar os eventos do ciclo de vida do AWS Control Tower para acionar funções do Lambda.

## Gerencie contas por meio de AWS Organizations

AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias AWS contas em uma organização que você cria e gerencia centralmente. Com o Organizations, você pode criar contas de membros e convidar contas existentes para se juntarem à sua organização. É possível organizar essas contas em grupos e anexar controles com base em políticas. Para obter mais informações, consulte o Guia do usuário do AWS Organizations.

No AWS Control Tower, o Organizations ajuda a gerenciar centralmente o faturamento; controlar o acesso, a conformidade e a segurança; e compartilhar recursos entre suas contas de membros AWS . As contas são agrupadas em grupos lógicos, chamados de unidades organizacionais (UOs). Para obter mais informações sobre Organizations, consulte o Guia AWS Organizations do Usuário.

O AWS Control Tower usa as seguintes OUs:

- Root — O contêiner principal para todas as contas e todas as outras OUs em sua landing zone.
- Segurança — Essa OU contém a conta de arquivamento de registros, a conta de auditoria e os recursos que ela possui.
- Sandbox — Essa OU é criada quando você configura sua landing zone. Ela e outras OUs secundárias em sua landing zone contêm suas contas de membro. Essas são as contas que seus usuários finais acessam para realizar trabalhos em AWS recursos.

> **Note**
>
> Você pode adicionar outras OUs em sua landing zone por meio do console do AWS Control Tower na página de unidades organizacionais.

### Considerações

As OUs criadas por meio do AWS Control Tower podem ter controles aplicados a elas. As OUs criadas fora do AWS Control Tower não podem, por padrão. No entanto, você pode registrar essas OUs. Depois de registrar uma OU, você pode aplicar controles a ela e a suas contas. Para obter informações sobre o registro de uma OU, consulte Registrar uma unidade organizacional existente no AWS Control Tower.

## Armazene objetos com o Amazon S3

O Amazon Simple Storage Service (Amazon S3) é armazenamento para a Internet. Você pode utilizar o Amazon S3 para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na web. Você pode realizar essas tarefas usando a interface da web simples e intuitiva do AWS Management Console. Para obter mais detalhes, consulte o Guia do usuário do Amazon Simple Storage Service.

Quando você configura sua landing zone, um bucket Amazon S3 é criado em sua conta de arquivamento de logs para conter todos os registros de todas as contas em sua landing zone.

## Monitore seu ambiente com o Security Hub

O AWS Control Tower é integrado ao AWS Security Hub por meio do padrão Security Hub chamado Service-Managed Standard: AWS Control Tower. Para obter mais informações, consulte Padrão do Security Hub.

## Provisione contas por meio de AWS Service Catalog

AWS Service Catalog permite que os administradores de TI criem, gerenciem e distribuam portfólios de produtos aprovados aos usuários finais, que então têm acesso aos produtos de que precisam em um portal personalizado. Os produtos típicos incluem servidores, bancos de dados, sites ou aplicativos que são implantados usando AWS recursos.

Você pode controlar os usuários que têm acesso a produtos específicos, o que permite impor a conformidade com os padrões de negócios organizacionais, gerenciar os ciclos de vida dos produtos e ajudar os usuários a encontrar e lançar produtos com confiança. Para obter mais informações, consulte o Service Catalog Administrator Guide.

No AWS Control Tower, seus administradores de nuvem central e seus usuários finais podem provisionar contas personalizadas em sua landing zone usando AWS Service Catalog produtos, chamados de “blueprints personalizados”. Para obter mais informações, consulte a Etapa 2. Crie o AWS Service Catalog produto.

O AWS Control Tower também pode usar as APIs do Service Catalog para automatizar ainda mais o provisionamento e a atualização de contas. Para obter detalhes, consulte o Guia do AWS Service Catalog desenvolvedor.

## Transição para o tipo de produto AWS Service Catalog externo

AWS Service Catalog alterou o suporte para produtos Terraform Open Source e produtos provisionados para um novo tipo de produto, chamado Externo. Para saber mais sobre essa transição, consulte Atualização dos produtos existentes do Terraform Open Source e dos produtos provisionados para o tipo de produto externo no guia do administrador.AWS Service Catalog

Essa alteração afeta as contas existentes que você criou ou inscreveu com a personalização de fábrica de contas do AWS Control Tower. Para fazer a transição dessas contas para o tipo de produto externo, você precisa fazer alterações tanto no AWS Control Tower AWS Service Catalog quanto no AWS Control Tower.

Para fazer a transição para o tipo de produto externo

1. Atualize seu Terraform Reference Engine existente AWS Service Catalog para incluir suporte para os tipos de produtos externos e de código aberto do Terraform. Para obter instruções sobre como atualizar seu Terraform Reference Engine, consulte o AWS Service Catalog GitHub Repositório.
2. Em AWS Service Catalog, duplique todos os produtos existentes do Terraform Open Source (blueprints), com as duplicatas usando o novo tipo de produto externo. Não encerre os blueprints existentes do Terraform Open Source.
3. No AWS Control Tower, atualize cada conta usando um plano de código aberto do Terraform para usar o novo plano externo.

a. Para atualizar um blueprint, você deve primeiro remover completamente o blueprint do Terraform Open Source. Para obter mais detalhes, consulte Remover um blueprint de uma conta.

b. Adicione o novo blueprint externo à mesma conta. Para obter mais detalhes, consulte Adicionar um modelo a uma conta do AWS Control Tower.

4. Depois que todas as contas que usam os blueprints do Terraform Open Source forem atualizadas para os blueprints externos, retorne AWS Service Catalog e encerre todos os produtos que usam o Terraform Open Source como tipo de produto.

5. No futuro, todas as contas criadas ou inscritas usando a personalização de fábrica de contas do AWS Control Tower devem fazer referência a esquemas usando o tipo de produto externo AWS CloudFormationou o tipo de produto.

   Para esquemas criados usando o tipo de produto externo, o AWS Control Tower suporta apenas personalizações de contas que usam modelos do Terraform e o mecanismo de referência do Terraform. Para saber mais, consulte Configurar para personalização.

> **Note**
>
> O AWS Control Tower não oferece suporte ao Terraform Open Source como um tipo de produto ao criar novas contas. Para saber mais sobre essas mudanças, consulte Atualização dos produtos existentes do Terraform Open Source e dos produtos provisionados para o tipo de produto externo no guia do administrador.AWS Service Catalog  AWS Service Catalog apoiará os clientes nessa transição de tipo de produto, conforme necessário. Entre em contato com o representante da sua conta para solicitar assistência.

## Rastreie alertas por meio do Amazon Simple Notification Service

O Amazon Simple Notification Service (Amazon SNS) é um serviço web que permite que aplicativos, usuários finais e dispositivos enviem e recebam notificações instantaneamente da nuvem. Para obter mais informações, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

O AWS Control Tower usa o Amazon SNS para enviar alertas programáticos para os endereços de e-mail da sua conta de gerenciamento e da sua conta de auditoria. Esses alertas ajudam você a evitar desvios dentro da sua landing zone. Para ter mais informações, consulte Detecte e resolva desvios na AWS Control Tower.

Também usamos o Amazon Simple Notification Service para enviar notificações de conformidade de AWS Config.

> **Tip**
>
> Uma das melhores maneiras de receber notificações de conformidade de controle do AWS Control Tower (em sua conta de auditoria) é se inscrever em`AggregateConfigurationNotifications`. É um serviço que ajuda você a inspecionar a conformidade. Ele fornece dados reais sobre AWS Config regras que estão fora de conformidade. AWS Config mantém automaticamente a lista de contas em sua OU. Você deve se inscrever manualmente, usando e-mail ou qualquer tipo de assinatura que o SNS permita. O extrato `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` leva à sua conta de auditoria.

## Crie aplicativos distribuídos com AWS Step Functions

AWS Step Functions facilita a coordenação dos componentes de aplicativos distribuídos como uma série de etapas em um fluxo de trabalho visual. Você pode criar e executar rapidamente máquinas de estado para executar as etapas de um aplicativo de forma confiável e escalável. Para obter mais informações, consulte o Guia do desenvolvedor do AWS Step Functions.

# Gerenciamento de identidade e acesso na AWS Control Tower

Para realizar qualquer operação em sua landing zone, como provisionar contas no Account Factory ou criar novas unidades organizacionais (OUs) no console da AWS Control Tower, AWS Identity and Access Management (IAM) ou AWS IAM Identity Center exigem que você autentique que é aprovado AWS usuário. Por exemplo, se você estiver usando o console AWS Control Tower, autentica sua identidade fornecendo seu AWS credenciais, conforme fornecidas pelo administrador.

Depois de autenticar sua identidade, IAM controla seu acesso a AWS com um conjunto definido de permissões em um conjunto específico de operações e recursos. Se você for administrador da conta, poderá usar IAM para controlar o acesso de outros IAM usuários aos recursos associados à sua conta.

Tópicos



## Autenticação

Você tem acesso a AWS como qualquer um dos seguintes tipos de identidades:

- AWS usuário raiz da conta — Quando você cria uma conta pela primeira vez AWS conta, você começa com uma identidade que tem acesso completo a todos AWS serviços e recursos na conta. Essa identidade é chamada de AWS usuário raiz da conta. Você tem acesso a essa identidade ao fazer login com o endereço de e-mail e a senha usados para criar a conta. É recomendável não usar o usuário raiz para suas tarefas diárias, nem mesmo para as administrativas. Em vez disso, adote a prática recomendada de usar o usuário root somente para criar seu primeiro usuário (recomendado) ou IAM usuário do IAM Identity Center (não é uma prática recomendada na maioria dos casos de uso). Depois, guarde as credenciais do usuário raiz em um lugar seguro e utilize-as

para executar somente algumas tarefas de gerenciamento de contas e serviços. Para obter mais informações, consulte Quando fazer login como usuário root.

- IAMusuário — Um IAMusuário é uma identidade dentro do seu AWS conta que tem permissões específicas e personalizadas. Você pode usar as credenciais IAM do usuário para fazer login e proteger AWS páginas da web como o AWS Console de gerenciamento, AWS Fóruns de discussão ou o AWS Support Center. AWS as melhores práticas recomendam que você crie um usuário do IAM Identity Center em vez de um IAM usuário, porque há mais risco de segurança ao criar um IAM usuário com credenciais de longo prazo.

  Se você precisar criar um IAM usuário para uma determinada finalidade, além das credenciais de login, poderá gerar chaves de acesso para cada usuário. IAM Você pode usar essas teclas ao ligar AWS serviços programaticamente, seja por meio de um dos vários SDKs ou usando o AWS Interface de linha de comando (CLI). As CLI ferramentas SDK e usam as chaves de acesso para assinar criptograficamente sua solicitação. Se você não usa AWS ferramentas, você mesmo deve assinar a solicitação. AWSO Control Tower oferece suporte ao Signature Version 4, um protocolo para autenticar solicitações de entradaAPI. Para obter mais informações sobre a autenticação de solicitações, consulte Processo de assinatura da versão 4 no AWS Referência geral.

- IAMfunção — Uma IAMfunção é uma IAM identidade que você pode criar em sua conta com permissões específicas. Uma IAM função é semelhante a de um IAM usuário, pois é uma AWS identidade, e tem políticas de permissões que determinam o que a identidade pode ou não fazer em AWS. No entanto, em vez de ser associada exclusivamente a uma pessoa, uma função deve ser assumida por qualquer pessoa que precise dela. Além disso, um perfil não tem credenciais de longo prazo padrão associadas a ele, como senha ou chaves de acesso. Em vez disso, quando você assumir um perfil, ele fornecerá credenciais de segurança temporárias para sua sessão de perfil. IAMfunções com credenciais temporárias são úteis nas seguintes situações:

  - Acesso de usuário federado — Em vez de criar um IAM usuário, você pode usar identidades existentes de AWS Directory Service, seu diretório de usuários corporativos ou um provedor de identidade na web. Estes são conhecidos como usuários federados. AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidade. Para obter mais informações sobre usuários federados, consulte Usuários e funções federados no Guia do IAMusuário.
  - AWS acesso ao serviço — Uma função de serviço é uma IAM função que um serviço assume para realizar ações em sua conta em seu nome. Quando você configura alguns AWS ambientes de serviço, você deve definir uma função a ser assumida pelo serviço. Essa função de serviço deve incluir todas as permissões necessárias para que o serviço acesse o AWS recursos de que precisa. As funções de serviço variam de acordo com o serviço, mas muitas permitem que você

escolha suas permissões, desde que atenda aos requisitos documentados para esse serviço. As funções de serviço fornecem acesso apenas dentro de sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Você pode criar, modificar e excluir uma função de serviço de dentroIAM. Por exemplo, é possível criar uma função que permita ao Amazon Redshift acessar um bucket do Amazon S3 em seu nome e carregar dados do bucket em um cluster do Amazon Redshift. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS Serviço no Guia do IAM Usuário.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância da Amazon e criando AWS CLIou AWS APIsolicitações. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância da Amazon. Para atribuir um AWS Ao atribuir uma função a uma EC2 instância da Amazon e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância que é anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância da Amazon obtenham credenciais temporárias. Para obter mais informações, consulte Usando uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

- IAMA autenticação do usuário do IAM Identity Center no portal do usuário do Identity Center é controlada pelo diretório que você conectou ao IAM Identity Center. No entanto, autorização para o AWS as contas que estão disponíveis para usuários finais a partir do portal do usuário são determinadas por dois fatores:
  - A quem foi atribuído acesso a esses AWS contas no AWS IAMConsole do Identity Center. Para obter mais informações, consulte Acesso ao Single Sign-On no AWS IAM Identity Center Guia do usuário.
  - Que nível de permissões foi concedido aos usuários finais no AWS IAMConsole do Identity Center para permitir que eles tenham o acesso apropriado a esses AWS contas. Para obter mais informações, consulte Conjuntos de permissões no AWS IAM Identity Center Guia do usuário.

# Controle de acesso

Para criar, atualizar, excluir ou listar recursos da AWS Control Tower ou outros AWS recursos em sua landing zone, você precisa de permissões para realizar a operação e precisa de permissões para acessar os recursos correspondentes. Além disso, para realizar a operação de forma programática, você precisa de chaves de acesso válidas.

As seções a seguir descrevem como gerenciar as permissões do AWS Control Tower:

Tópicos

- Visão geral do gerenciamento de permissões de acesso aos recursos da AWS Control Tower
- Usando políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower

# Trabalhando com o AWS IAM Identity Center e o AWS Control Tower

No AWS Control Tower, o IAM Identity Center permite que administradores centrais de nuvem e usuários finais gerenciem o acesso a várias AWS contas e aplicativos comerciais. Por padrão, o AWS Control Tower usa esse serviço para configurar e gerenciar o acesso às contas criadas por meio do Account Factory, a menos que você tenha selecionado a opção de autogerenciar sua identidade e controle de acesso.

Para obter mais informações sobre como selecionar um provedor de identidade, consulteIAMOrientação do Identity Center.

Para ver um breve tutorial sobre como configurar seus usuários e permissões do IAM Identity Center no AWS Control Tower, você pode assistir a este vídeo (6:23). Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Vídeo passo a passo da configuração do AWS IAM Identity Center no AWS Control Tower.

Sobre a configuração do AWS Control Tower com o IAM Identity Center

Quando você configura inicialmente o AWS Control Tower, somente o usuário raiz e qualquer usuário do IAM com as permissões corretas podem adicionar usuários do IAM Identity Center. No entanto, depois que os usuários finais forem adicionados ao AWSAccountFactorygrupo, eles poderão criar novos usuários do IAM Identity Center usando o assistente Account Factory. Para ter mais informações, consulte Provisione e gerencie contas com o Account Factory.

Se você escolher o padrão recomendado, o AWS Control Tower configura sua landing zone com um diretório pré-configurado que ajuda você a gerenciar identidades de usuário e login único, para que seus usuários tenham acesso federado em todas as contas. Quando você configura sua landing zone, esse diretório padrão é criado para conter grupos de usuários e conjuntos de permissões.

> **Note**
>
> Você pode delegar a administração da AWS IAM Identity Center sua organização a uma conta diferente da conta de gerenciamento, usando o recurso de administrador delegado do IAM Identity Center. Se você optar por usar esse recurso, saiba que os administradores com acesso para gerenciar a associação ao grupo também podem gerenciar grupos atribuídos à conta de gerenciamento. Para obter mais informações, consulte esta postagem no blog, intitulada Introdução à administração delegada do AWS SSO

## Grupos de usuários, funções e conjuntos de permissões

Os grupos de usuários gerenciam funções especializadas definidas nas contas compartilhadas. As funções estabelecem conjuntos de permissões que pertencem umas às outras. Todos os membros de um grupo herdam os conjuntos de permissões, ou funções, associados ao grupo. É possível criar novos grupos para os usuários finais das contas-membro para que você possa atribuir apenas as funções necessárias às tarefas específicas executadas pelo grupo.

Os conjuntos de permissões disponíveis abrangem uma ampla variedade de requisitos de permissão de usuário distintos, como acesso somente leitura, acesso administrativo ao AWS Control Tower e acesso ao Service Catalog. Esses conjuntos de permissões permitem que seus usuários finais provisionem suas próprias AWS contas em seu landing zone rapidamente e em conformidade com as diretrizes da sua empresa.

Para obter dicas sobre como planejar suas alocações de usuários, grupos e permissões, consulte Recomendações para configurar grupos, funções e políticas

Para obter mais informações sobre como usar esse serviço no contexto do AWS Control Tower, consulte os tópicos a seguir no Guia doAWS IAM Identity Center usuário.

- Para adicionar usuários, consulte Adicionar usuários.
- Para adicionar usuários a grupos, consulte Adicionar usuários a grupos.
- Para editar propriedades do usuário, consulte Editar propriedades do usuário.
- Para adicionar um grupo, consulte Adicionar grupos.

> **Warning**
>
> O AWS Control Tower configura seu diretório do IAM Identity Center em sua região de origem. Se você configurar sua landing zone em outra região e depois navegar até o console do IAM Identity Center, deverá alterar a região para sua região de origem. Não exclua a configuração do IAM Identity Center em sua região de origem.

## Coisas que você deve saber sobre as contas do IAM Identity Center e o AWS Control Tower

Aqui estão algumas coisas boas que você deve saber ao trabalhar com contas de usuário do IAM Identity Center no AWS Control Tower.

- Se sua conta de usuário do AWS IAM Identity Center estiver desativada, você receberá uma mensagem de erro ao tentar provisionar novas contas no Account Factory. Você pode reativar seu usuário do IAM Identity Center no console do IAM Identity Center.
- Se você especificar um novo endereço de e-mail de usuário do IAM Identity Center ao atualizar o produto provisionado associado a uma conta vendida pela Account Factory, o AWS Control Tower cria uma nova conta de usuário do IAM Identity Center. A conta de usuário criada anteriormente não será removida. Se você preferir remover o endereço de e-mail anterior do usuário do IAM Identity Center do AWS IAM Identity Center, consulte Desabilitar um usuário.
- AWS O IAM Identity Center foi integrado ao Azure Active Directory, e você pode conectar seu Azure Active Directory existente ao AWS Control Tower.
- Para obter mais informações sobre como o comportamento do AWS Control Tower interage com o AWS IAM Identity Center e diferentes fontes de identidade, consulte Considerations for Changing Your Identity Source na documentação do AWS IAM Identity Center.

## Grupos do IAM Identity Center para o AWS Control Tower

O AWS Control Tower oferece grupos pré-configurados para organizar usuários que realizam tarefas específicas em suas contas. Você pode adicionar usuários e atribuí-los a esses grupos diretamente no IAM Identity Center. Isso corresponde a conjuntos de permissões para usuários em grupos dentro das contas. Os grupos a seguir são criados quando você configura sua landing zone.

AWSAccountFactory

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de gerenciamento | AWSServiceCatalogEndUserAccess | Esse grupo só é usado nessa conta para provisionar novas contas usando o Account Factory. |

AWSServiceCatalogAdmins

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de gerenciamento | AWSServiceCatalogAdminFullAccess | Esse grupo só é usado nessa conta para fazer alterações administrativas no Account Factory. Os usuários desse grupo não podem provisionar novas contas, a menos que também estejam no AWSAccountFactorygrupo. |

AWSControlTowerAdmins

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de gerenciamento | AWSAdministratorAccess | Os usuários desse grupo nessa conta são os únicos que têm acesso ao console do AWS Control Tower. |
| Conta de arquivamento de logs | AWSAdministratorAccess | Os usuários dessa conta têm acesso de administrador. |
| Conta de auditoria | AWSAdministratorAccess | Os usuários dessa conta têm acesso de administrador. |

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Contas-membro | AWSOrganizationsFullAccess | Os usuários têm acesso total às Organizations nessa conta. |

AWSSecurityAuditPowerUsers

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de gerenciamento | AWSPowerUserAccess | Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configurar recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativos. |
| Conta de arquivamento de logs | AWSPowerUserAccess | Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configurar recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativos. |
| Conta de auditoria | AWSPowerUserAccess | Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configurar recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativos. |
| Contas-membro | AWSPowerUserAccess | Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configurar recursos e serviços que |

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| | | suportem o desenvolvimento AWS consciente de aplicativos. |

AWSSecurityAuditors

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de gerenciamento | AWSReadOnlyAccess | Os usuários têm acesso somente de leitura a todos os AWS serviços e recursos dessa conta. |
| Conta de arquivamento de logs | AWSReadOnlyAccess | Os usuários têm acesso somente de leitura a todos os AWS serviços e recursos dessa conta. |
| Conta de auditoria | AWSReadOnlyAccess | Os usuários têm acesso somente de leitura a todos os AWS serviços e recursos dessa conta. |
| Contas-membro | AWSReadOnlyAccess | Os usuários têm acesso somente de leitura a todos os AWS serviços e recursos dessa conta. |

AWSLogArchiveAdmins

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de arquivamento de logs | AWSAdministratorAccess | Os usuários dessa conta têm acesso de administrador. |

AWSLogArchiveViewers

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de arquivamento de logs | AWSReadOnlyAccess | Os usuários têm acesso somente de leitura a todos os AWS serviços e recursos dessa conta. |

AWSAuditAccountAdmins

| Conta | Conjuntos de permissões | Descrição |
| --- | --- | --- |
| Conta de auditoria | AWSAdministratorAccess | Os usuários dessa conta têm acesso de administrador. |

# Visão geral do gerenciamento de permissões de acesso aos recursos da AWS Control Tower

Cada AWS o recurso é de propriedade de um Conta da AWS, e as permissões para criar ou obter acesso a um recurso são regidas por políticas de permissões. Um administrador da conta pode anexar políticas de permissões às IAM identidades (ou seja, usuários, grupos e funções). Alguns serviços (como AWS Lambda) também oferecem suporte para anexar políticas de permissões aos recursos.

> **Note**
>
> Um administrador da conta (ou administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte as IAM melhores práticas no Guia IAM do usuário.

Quando você é responsável por conceder permissões a um usuário ou função, deve conhecer e monitorar os usuários e funções que exigem permissões, os recursos para os quais cada usuário e função exigem permissões e as ações específicas que devem ser permitidas para operar esses recursos.

Tópicos

## AWSRecursos e operações da Control Tower

Na AWS Control Tower, o recurso principal é uma landing zone. AWSO Control Tower também suporta um tipo de recurso adicional, os controles, às vezes chamados de grades de proteção. No entanto, para o AWS Control Tower, você pode gerenciar controles somente no contexto de uma landing zone existente. Os controles podem ser chamados de sub-recursos.

Recursos e sub-recursos em AWS têm nomes de recursos exclusivos da Amazon (ARNs) associados a eles, conforme mostrado no exemplo a seguir.

AWSA Control Tower fornece um conjunto de API operações para trabalhar com os recursos da AWS Control Tower. Para obter uma lista das operações disponíveis, consulte AWS Control Tower the AWS Control Tower API Reference.

Para obter mais informações sobre o AWS CloudFormation recursos no AWS Control Tower, veja o AWS CloudFormation Guia do usuário.

## Sobre a propriedade de recursos

A ferramenta AWS A conta possui os recursos que são criados na conta, independentemente de quem criou os recursos. Especificamente, o proprietário do recurso é o AWS conta da entidade principal (ou seja, o Conta da AWS usuário raiz, um usuário do IAM Identity Center, um IAM usuário ou uma IAM função) que autentica a solicitação de criação do recurso. Os seguintes exemplos mostram como isso funciona:

- Se você usar o AWS credenciais de usuário raiz da conta do seu AWS conta para configurar uma landing zone, sua AWS a conta é a proprietária do recurso.
- Se você criar um IAM usuário no seu AWS conta e conceda permissões para configurar uma zona de pouso para esse usuário, o usuário pode configurar uma zona de pouso, desde que sua conta atenda aos pré-requisitos. No entanto, seu AWS A conta, à qual o usuário pertence, é proprietária do recurso landing zone.

- Se você criar uma IAM função em seu AWS conta com permissões para configurar uma zona de pouso, qualquer pessoa que possa assumir a função pode configurar uma zona de pouso. Suas AWS A conta, à qual a função pertence, é proprietária do recurso landing zone.

## Gerencie o acesso aos recursos

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação das políticas de permissões.

> **Note**
>
> Esta seção discute o uso IAM no contexto do AWS Control Tower. Ele não fornece informações detalhadas sobre o IAM serviço. Para obter a IAM documentação completa, consulte O que éIAM? no Guia do IAM usuário. Para obter informações sobre a sintaxe e as descrições da IAM política, consulte AWS IAMReferência de política no Guia IAM do usuário.

As políticas anexadas a uma IAM identidade são chamadas de políticas baseadas em identidade (IAMpolíticas). As políticas anexadas a um recurso são chamadas de políticas baseadas em recursos.

> **Note**
>
> AWSO Control Tower oferece suporte somente a políticas baseadas em identidade (IAMpolíticas).

Tópicos

- Sobre políticas baseadas em identidade (políticas) IAM
- Crie funções e atribua permissões
- Políticas baseadas no recurso

### Sobre políticas baseadas em identidade (políticas) IAM

Você pode anexar políticas às IAM identidades. Por exemplo, você pode fazer o seguinte:

- Anexe uma política de permissões a um usuário ou grupo em sua conta — Para conceder a um usuário permissões para criar um recurso do AWS Control Tower, como configurar uma landing zone, você pode anexar uma política de permissões a um usuário ou grupo ao qual o usuário pertence.
- Anexar uma política de permissões a uma função (conceder permissões entre contas) — Você pode anexar uma política de permissões baseada em identidade a uma IAM função para conceder permissões entre contas. Por exemplo, um administrador para um AWS a conta (Conta A) pode criar uma função que concede permissões entre contas a outra AWS conta (Conta B), ou o administrador pode criar uma função que conceda permissões a outra AWS serviço.
  1. O administrador da Conta A cria uma IAM função e anexa uma política de permissões à função que concede permissões para gerenciar recursos na Conta A.
  2. O administrador da Conta A atribui uma política de confiança à função. A política identifica a conta B como a entidade principal que pode assumir a função.
  3. Como principal, o administrador da Conta B pode dar permissão a qualquer usuário da Conta B para assumir a função. Ao assumir a função, os usuários na Conta B podem criar ou obter acesso aos recursos na Conta A.
  4. Para conceder um AWS serviço a capacidade (permissões) de assumir a função, o principal que você especifica na política de confiança pode ser um AWS serviço.

## Crie funções e atribua permissões

Funções e permissões dão acesso a recursos, na AWS Control Tower e em outros AWS serviços, incluindo acesso programático aos recursos.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criar um conjunto de permissões no AWS IAM Identity Center Guia do usuário.
- Usuários gerenciados IAM por meio de um provedor de identidade:

  Crie um perfil para a federação de identidades. Siga as instruções em Criação de uma função para um provedor de identidade terceirizado (federação) no Guia IAM do usuário.
- IAMusuários:

- Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de uma função para um IAM usuário no Guia IAM do usuário.
- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adicionar permissões a um usuário (console) no Guia do IAM usuário.

Para obter mais informações sobre IAM como delegar permissões, consulte Gerenciamento de acesso no Guia do IAM usuário.

> **Note**
>
> Ao configurar uma landing zone da AWS Control Tower, você precisará de um usuário ou função com a política AdministratorAccessgerenciada. (arn:aws:iam: :aws:policy/) AdministratorAccess

Para criar uma função para um AWS service (Serviço da AWS) (IAMconsole)

1. Faça login no AWS Management Console e abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação do IAM console, escolha Funções e, em seguida, escolha Criar função.
3. Para Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
4. Para Serviço ou caso de uso, escolha um serviço e, em seguida, escolha o caso de uso. Casos de uso são definidos pelo serviço para incluir a política de confiança exigida pelo serviço.
5. Escolha Próximo.
6. As opções para Políticas de permissões dependem do caso de uso selecionado.
   - Se o serviço definir as permissões para o perfil, não será possível selecionar políticas de permissões.
   - Selecione em um conjunto limitado de políticas de permissões.
   - Selecione entre todas as políticas de permissões.
   - Não selecione nenhuma política de permissão; crie políticas após a criação do perfil e, em seguida, anexe as políticas ao perfil.
7. (Opcional) Defina um limite de permissões. Esse é um atributo avançado que está disponível para perfis de serviço, mas não para perfis vinculados ao serviço.

a. Abra a seção Definir limite de permissões e escolha Usar um limite de permissões para controlar o número máximo de permissões do perfil.

   IAMinclui uma lista dos AWS políticas gerenciadas e gerenciadas pelo cliente em sua conta.

b. Selecione a política a ser usada para o limite de permissões.

8. Escolha Próximo.
9. Para Nome do perfil, as opções dependem do serviço:

   - Se o serviço definir o nome do perfil, não será possível editar esse nome.
   - Se o serviço definir um prefixo para o nome do perfil, você poderá inserir um sufixo opcional.
   - Se o serviço definir o nome do perfil, você poderá atribuir um nome ao perfil.

   > **Important**
   >
   > Quando nomear um perfil, observe o seguinte:
   >
   > - Os nomes das funções devem ser exclusivos em seu Conta da AWS, e não pode ser tornada única caso a caso.
   >
   >   Por exemplo, não crie dois perfis denominados **`PRODROLE`** e **`prodrole`**. Quando um nome de função é usado em uma política ou como parte de umaARN, o nome da função diferencia maiúsculas de minúsculas, no entanto, quando um nome de função aparece para os clientes no console, como durante o processo de login, o nome da função não diferencia maiúsculas de minúsculas.
   > - Não é possível editar o nome do perfil depois de criá-lo porque outras entidades podem referenciar o perfil.

10. (Opcional) Em Descrição, insira uma descrição para o perfil.
11. (Opcional) Para editar os casos de uso e as permissões do perfil, escolha Editar nas seções Etapa 1: selecionar entidades confiáveis ou Etapa 2: adicionar permissões.
12. (Opcional) Para ajudar a identificar, organizar ou pesquisar o perfil, adicione tags como pares de chave-valor. Para obter mais informações sobre o uso de tags emIAM, consulte IAMRecursos de marcação no Guia do IAM usuário.
13. Reveja a função e escolha Criar função.

Para usar o editor JSON de políticas para criar uma política

1. Faça login no AWS Management Console e abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Policies (Políticas).

   Se essa for a primeira vez que você escolhe Políticas, a página Bem-vindo às políticas gerenciadas será exibida. Escolha Começar.
3. Na parte superior da página, escolha Criar política.
4. Na seção Editor de políticas, escolha a JSONopção.
5. Insira ou cole um documento JSON de política. Para obter detalhes sobre a linguagem da IAM política, consulte a referência IAM JSON da política.
6. Resolva os avisos de segurança, erros ou avisos gerais gerados durante a validação de política e depois escolha Próximo.

   > **Note**
   >
   > Você pode alternar entre as opções Visual e JSONEditor a qualquer momento. No entanto, se você fizer alterações ou escolher Avançar no editor visual, IAM poderá reestruturar sua política para otimizá-la para o editor visual. Para obter mais informações, consulte Reestruturação de políticas no Guia do IAM usuário.
7. (Opcional) Quando você cria ou edita uma política no AWS Management Console, você pode gerar um modelo YAML de política JSON ou que você pode usar no AWS CloudFormation modelos.

   Para fazer isso, no editor de políticas, escolha Ações e, em seguida, escolha Gerar CloudFormation modelo. Para saber mais a respeito AWS CloudFormation, veja AWS Identity and Access Management referência de tipo de recurso no AWS CloudFormation Guia do usuário.
8. Quando terminar de adicionar as permissões à política, escolha Avançar.
9. Na página Revisar e criar, insira um Nome de política e uma Descrição (opcional) para a política que você está criando. Revise Permissões definidas nessa política para ver as permissões que são concedidas pela política.

10. (Opcional) Adicione metadados à política associando tags como pares de chave-valor. Para obter mais informações sobre o uso de tags emIAM, consulte IAMRecursos de marcação no Guia do IAM usuário.
11. Escolha Criar política para salvar sua nova política.

Para usar o editor visual para criar uma política

1. Faça login no AWS Management Console e abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha Policies (Políticas).

   Se essa for a primeira vez que você escolhe Políticas, a página Bem-vindo às políticas gerenciadas será exibida. Escolha Começar.
3. Escolha Criar política.
4. Na seção Editor de políticas, localize a seção Selecionar um serviço e, em seguida, escolha um AWS service (Serviço da AWS). Você pode usar a caixa de pesquisa na parte superior para limitar os resultados na lista de serviços. Você pode escolher apenas um serviço em um bloco de permissões no editor visual. Para conceder acesso a mais de um serviço, adicione vários blocos de permissões escolhendo Adicionar mais permissões.
5. Em Ações permitidas, escolha as ações a serem adicionadas à política. Você pode escolher as ações das seguintes maneiras:

   - Marque a caixa de seleção para todas as ações.
   - Escolha Adicionar ações para inserir o nome de uma ação específica. Você pode usar um caractere curinga (*) para especificar várias ações.
   - Selecione um dos grupos de Nível de acesso para escolher todas as ações do nível de acesso (por exemplo, Leitura, Gravação ou Lista).
   - Expanda cada um dos grupos de Access level para escolher as ações individuais.

   Por padrão, a política que você está criando permite as ações que você escolhe. Para negar as ações escolhidas, selecione Alternar para negar permissões. Como IAMnega por padrão, recomendamos, como prática recomendada de segurança, que você conceda permissões somente para as ações e recursos de que o usuário precisa. Crie uma JSON declaração para negar permissões somente se você quiser substituir uma permissão permitida separadamente por outra declaração ou política. Recomendamos que você limite ao mínimo o número de

permissões de negação, pois elas podem aumentar a dificuldade de solucionar problemas nas permissões.

6. Para Recursos, se o serviço e as ações que você selecionou nas etapas anteriores não oferecerem suporte à escolha de recursos específicos, todos os recursos serão permitidos e você não poderá editar esta seção.

   Se você escolher uma ou mais ações que ofereçam suporte a permissões no nível de recursos, o editor visual listará esses recursos. Você poderá expandir Recursos para especificar os recursos para sua política.

   É possível especificar recursos das seguintes maneiras:

   - Escolha Adicionar ARNs para especificar recursos por seus nomes de recursos da Amazon (ARN). Você pode usar o ARN editor visual ou a lista ARNs manualmente. Para obter mais informações sobre ARN sintaxe, consulte Amazon Resource Names (ARNs) no Guia do IAM usuário. Para obter informações sobre o uso ARNs no `Resource` elemento de uma política, consulte elementos IAM JSON da política: Recurso no Guia IAM do usuário.
   - Escolha Qualquer um nesta conta ao lado de um recurso para conceder permissões a qualquer recurso desse tipo.
   - Escolha Todos os recursos para escolher todos os recursos para o serviço.

7. (Opcional) Escolha Condições de solicitação - opcional para adicionar condições à política que você está criando. As condições limitam o efeito JSON de uma declaração de política. Por exemplo, você pode especificar que um usuário só tem permissão para executar ações nos recursos quando sua solicitação ocorrer em um determinado período. Você também pode usar condições comumente usadas para limitar se um usuário deve ser autenticado usando um dispositivo de autenticação multifator (MFA). Ou você pode exigir que a solicitação tenha origem em um determinado intervalo de endereços IP. Para obter listas de todas as chaves de contexto que você pode usar em uma condição de política, consulte Ações, recursos e chaves de condição para AWS serviços na Referência de Autorização de Serviço.

   Você pode escolher as condições das seguintes maneiras:

   - Use as caixas de seleção para selecionar as condições comumente utilizadas.
   - Escolha Adicionar outra condição para especificar outras condições. Escolha a Chave de Condição, o Qualificador e o Operador da condição e, em seguida, insira um Valor. Para adicionar mais de um valor, escolha Adicionar. Você pode considerar os valores como conectados por um `OR` operador lógico. Quando terminar, selecione Adicionar condição.

Para adicionar mais de uma condição, escolha novamente Adicionar outra condição. Repita conforme necessário. Cada condição se aplica apenas a um bloco de permissões do editor visual. Todas as condições devem ser verdadeiras para que o bloco de permissões seja considerado uma correspondência. Em outras palavras, considere as condições a serem conectadas por um AND operador lógico.

Para obter mais informações sobre o elemento Condição, consulte Elementos de IAM JSON política: Condição no Guia IAM do Usuário.

8. Para adicionar mais blocos de permissão, escolha Adicionar mais permissões. Para cada bloco, repita as etapas de 2 a 5.

> **Note**
>
> Você pode alternar entre as opções Visual e JSONEditor a qualquer momento. No entanto, se você fizer alterações ou escolher Avançar no editor visual, IAM poderá reestruturar sua política para otimizá-la para o editor visual. Para obter mais informações, consulte Reestruturação de políticas no Guia do IAM usuário.

9. (Opcional) Quando você cria ou edita uma política no AWS Management Console, você pode gerar um modelo YAML de política JSON ou que você pode usar no AWS CloudFormation modelos.

   Para fazer isso, no editor de políticas, escolha Ações e, em seguida, escolha Gerar CloudFormation modelo. Para saber mais a respeito AWS CloudFormation, veja AWS Identity and Access Management referência de tipo de recurso no AWS CloudFormation Guia do usuário.

10. Quando terminar de adicionar as permissões à política, escolha Avançar.
11. Na página Revisar e criar, insira um Nome de política e uma Descrição (opcional) para a política que você está criando. Revise Permissões definidas nessa política para ter certeza de que você concedeu as permissões que pretendia.
12. (Opcional) Adicione metadados à política associando tags como pares de chave-valor. Para obter mais informações sobre o uso de tags emIAM, consulte IAMRecursos de marcação no Guia do IAM usuário.
13. Escolha Criar política para salvar sua nova política.

Para conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| Identificação da força de trabalho<br><br>(Usuários gerenciados no IAM Identity Center) | Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI, AWS SDKs, ou AWS APIs. | Siga as instruções da interface que deseja utilizar.<br><br>• Para o AWS CLI, consulte Configurando o AWS CLI para usar AWS IAM Identity Center no AWS Command Line Interface Guia do usuário.<br>• Para AWS SDKs, ferramentas e AWS APIs, consulte Autenticação do IAM Identity Center no AWS SDKsGuia de referência de ferramentas e ferramentas. |
| IAM | Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI, AWS SDKs, ou AWS APIs. | Seguindo as instruções em Usando credenciais temporárias com AWS recursos no Guia do IAM usuário. |
| IAM | (Não recomendado)<br>Use credenciais de longo prazo para assinar solicitações programáticas para o | Siga as instruções da interface que deseja utilizar.<br><br>• Para o AWS CLI, consulte Autenticação usando credenciais de IAM usuário |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| | AWS CLI, AWS SDKs, ou AWS APIs. | no AWS Command Line Interface Guia do usuário.<br>• Para AWS SDKse ferramentas, consulte Autenticar usando credenciais de longo prazo no AWS SDKsGuia de referência de ferramentas e ferramentas.<br>• Para AWS APIs, consulte Gerenciamento de chaves de acesso para IAM usuários no Guia IAM do usuário. |

Proteja-se contra atacantes

Para obter mais informações sobre como ajudar a se proteger contra invasores ao conceder permissões a outros AWS diretores de serviço, consulte Condições opcionais para suas relações de confiança de função. Ao adicionar determinadas condições às suas políticas, você pode ajudar a evitar um tipo específico de ataque, conhecido como ataque adjunto confuso, que ocorre se uma entidade coagir uma entidade com mais privilégios a realizar uma ação, como a falsificação de identidade entre serviços. Para obter informações gerais sobre as condições da política, consulte tambémEspecificar condições em uma política.

Para obter mais informações sobre o uso de políticas baseadas em identidade com o AWS Control Tower, consulte. Usando políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Guia do IAM usuário.

## Políticas baseadas no recurso

Outros serviços, como o Amazon S3, também aceitam políticas de permissões baseadas em recurso. Por exemplo: você pode anexar uma política a um bucket do S3 para gerenciar permissões

de acesso a esse bucket. AWSA Control Tower não oferece suporte a políticas baseadas em recursos.

## Especifique os elementos da política: ações, efeitos e princípios

Você pode configurar e gerenciar sua zona de pouso por meio do console AWS Control Tower ou da zona de pouso APIs. Para configurar sua landing zone, você deve ser um IAM usuário com permissões administrativas, conforme definido em uma IAM política.

Os elementos a seguir são os mais básicos que você pode identificar em uma política:

- Recurso — Em uma política, você usa um Amazon Resource Name (ARN) para identificar o recurso ao qual a política se aplica. Para obter mais informações, consulte AWSRecursos e operações da Control Tower.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Para obter informações sobre os tipos de ações disponíveis para serem executadas, consulte Ações definidas pela AWS Control Tower.
- Efeito: você especifica o efeito quando o usuário solicita a ação específica, que pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Principal — Em políticas baseadas em identidade (IAMpolíticas), o usuário ao qual a política está vinculada é o principal implícito. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (isso se aplica somente a políticas baseadas em recursos). AWSA Control Tower não oferece suporte a políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições das IAM políticas, consulte AWS IAMReferência de política no Guia IAM do usuário.

## Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da IAM política para especificar as condições em que uma política deve entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre a especificação de condições em um idioma de política, consulte Condição no Guia do IAM Usuário.

Para expressar condições, você pode usar chaves de condição predefinidas. Não há chaves de condição específicas para a AWS Control Tower. No entanto, existem AWS-chaves de condição amplas que você pode usar conforme apropriado. Para obter uma lista completa de AWS-teclas largas, consulte Teclas disponíveis para ver as condições no Guia do IAM usuário.

## Evite a falsificação de identidade entre serviços

Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. Quando um serviço chama outro serviço, a falsificação de identidade entre serviços ocorre se um serviço manipula outro serviço para usar suas permissões para agir sobre os recursos do cliente de uma forma que não seria permitida de outra forma. Para evitar esse ataque, AWS fornece ferramentas para ajudar você a proteger seus dados, para que somente os serviços com permissão legítima possam ter acesso aos recursos da sua conta.

Recomendamos usar as `aws:SourceAccount` condições `aws:SourceArn` e em suas políticas para limitar as permissões que a AWS Control Tower concede a outro serviço para acessar seus recursos.

- Use `aws:SourceArn` se quiser que somente um recurso seja associado ao acesso entre serviços.
- Use `aws:SourceAccount` se quiser permitir que qualquer recurso dessa conta seja associado ao uso entre serviços.
- Se o `aws:SourceArn` valor não contiver o ID da conta, como o ARN de um bucket do Amazon S3, você deverá usar as duas condições para limitar as permissões.
- Se você usar as duas condições e se o `aws:SourceArn` valor contiver o ID da conta, o `aws:SourceAccount` valor e a conta no `aws:SourceArn` valor deverão mostrar o mesmo ID da conta quando usados na mesma declaração de política

Para ter mais informações e exemplos, consulte https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

# Usando políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower

Este tópico fornece exemplos de políticas baseadas em identidade que demonstram como um administrador de conta pode anexar políticas de permissões às identidades do IAM (ou seja,

usuários, grupos e funções) e, assim, conceder permissões para realizar operações nos recursos do AWS Control Tower.

> **Important**
>
> Recomendamos que você primeiro analise os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos seus recursos do AWS Control Tower. Para ter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos recursos da AWS Control Tower.

## Permissões necessárias para usar o console do AWS Control Tower

O AWS Control Tower cria três funções automaticamente quando você configura uma landing zone. Todas as três funções são necessárias para permitir o acesso ao console. O AWS Control Tower divide as permissões em três funções como melhor prática para restringir o acesso aos conjuntos mínimos de ações e recursos.

Três funções obrigatórias

- AWS ControlTowerAdmin papel
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Recomendamos que você restrinja o acesso às políticas de confiança de sua função para essas funções. Para obter mais informações, consulte Condições opcionais para as relações de confiança de sua função.

## AWS ControlTowerAdmin papel

Essa função fornece ao AWS Control Tower acesso à infraestrutura essencial para a manutenção da landing zone. A `AWS ControlTowerAdmin` função exige uma política gerenciada anexada e uma política de confiança de função para a função do IAM. Uma política de confiança de função é uma política baseada em recursos, especificando quais diretores podem assumir a função.

Aqui está um exemplo de trecho dessa política de confiança de funções:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para criar essa função a partir da AWS CLI e colocá-la em um arquivo chamado`trust.json`, veja um exemplo de comando da CLI:

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

Essa função exige duas políticas do IAM.

1. Uma política em linha, por exemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

2. A política gerenciada a seguir, que é `AWS ControlTowerServiceRolePolicy` a.

## AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicyÉ uma política AWS gerenciada que define permissões para criar e gerenciar recursos da AWS Control Tower, como AWS CloudFormation conjuntos de pilhas e instâncias de pilha, arquivos de AWS CloudTrail log, um agregador de configuração para a AWS Control Tower, bem como AWS Organizations contas e unidades organizacionais (OUs) que são governadas pela AWS Control Tower.

As atualizações dessa política gerenciada estão resumidas na tabela,Políticas gerenciadas para o AWS Control Tower.

Para obter mais informações, consulte o Guia *AWSControlTowerServiceRolePolicy*de referência de políticas gerenciadas da AWS.

Nome da política gerenciada: `AWS ControlTowerServiceRolePolicy`

O artefato JSON para `AWS ControlTowerServiceRolePolicy` é o seguinte:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
```

```
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
```

```
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

Política de confiança da função:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

A política em linha é`AWSControlTowerAdminPolicy`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

## AWS ControlTowerStackSetRole

AWS CloudFormation assume essa função para implantar conjuntos de pilhas em contas criadas pelo AWS Control Tower. Política em linha:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Política de confiança

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

## AWS ControlTowerCloudTrailRole

O AWS Control Tower habilita, CloudTrail como melhor prática, e fornece essa função para CloudTrail. CloudTrailassume essa função para criar e publicar CloudTrail registros. Política em linha:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

### Política de confiança

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

# AWSControlTowerBlueprintAccess requisitos de função

O AWS Control Tower exige que você crie a `AWSControlTowerBlueprintAccess` função na conta designada do blueprint hub, dentro da mesma organização.

Nome da função

O tipo de função deve ser `AWSControlTowerBlueprintAccess`.

Política de confiança de funções

A função deve ser configurada para confiar nos seguintes princípios:

- O diretor que usa o AWS Control Tower na conta de gerenciamento.
- A `AWSControlTowerAdmin` função na conta de gerenciamento.

O exemplo a seguir mostra uma política de confiança com privilégios mínimos. Ao criar sua própria política, substitua o termo *`YourManagementAccountId`*pelo ID real da conta de gerenciamento da sua conta de gerenciamento do AWS Control Tower e substitua o termo *`YourControlTowerUserRole`*pelo identificador da função do IAM para sua conta de gerenciamento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Permissões de função

Você deve anexar a política gerenciada AWSServiceCatalogAdminFullAccessà função.

## AWSServiceRoleForAWSControlTower

Essa função fornece ao AWS Control Tower acesso à conta do Log Archive, à conta de auditoria e às contas de membros para operações essenciais para a manutenção da landing zone, como notificar você sobre recursos desviados.

A `AWSServiceRoleForAWSControlTower` função exige uma política gerenciada anexada e uma política de confiança de função para a função do IAM.

Política gerenciada para essa função: `AWSControlTowerAccountServiceRolePolicy`

Política de confiança da função:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

## AWSControlTowerAccountServiceRolePolicy

Essa política AWS gerenciada permite que o AWS Control Tower chame AWS serviços que fornecem configuração automatizada de contas e governança centralizada em seu nome.

A política contém as permissões mínimas para a Torre de Controle da AWS implementar o encaminhamento de AWS Security Hub descobertas para recursos gerenciados pelos controles do Security Hub que fazem parte do padrão gerenciado pelo serviço do Security Hub: AWS Control Tower, e evita alterações que restringem a capacidade de gerenciar contas de clientes. É parte do processo de detecção de AWS Security Hub desvios em segundo plano que não é iniciado diretamente pelo cliente.

A política dá permissões para criar EventBridge regras da Amazon, especificamente para controles do Security Hub, em cada conta de membro, e essas regras devem especificar uma exata EventPattern. Além disso, uma regra pode operar somente em regras gerenciadas por nosso diretor de serviço.

Principal do serviço: `controltower.amazonaws.com`

O artefato JSON para `AWSControlTowerAccountServiceRolePolicy` é o seguinte:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
```

```
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "controltower.amazonaws.com"
     }
    }
   },
   // More managed rule permissions
   {
    "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
   },
   // Add permission to publish the security notifications to SNS
   {
    "Sid": "AllowControlTowerToPublishSecurityNotifications",
    "Effect": "Allow",
    "Action": "sns:publish",
    "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
    "Condition": {
     "StringEquals": {
      "aws:PrincipalAccount": "${aws:ResourceAccount}"
     }
    }
   },
   // For drift verification
   {
    "Sid": "AllowActionsForSecurityHubIntegration",
    "Effect": "Allow",
    "Action": [
     "securityhub:DescribeStandardsControls",
     "securityhub:GetEnabledStandards"
    ],
    "Resource": "arn:aws:securityhub:*:*:hub/default"
   }
  ]
}
```

As atualizações dessa política gerenciada estão resumidas na tabela,[Políticas gerenciadas para o AWS Control Tower](#).

# Políticas gerenciadas para o AWS Control Tower

AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela AWS. As políticas gerenciadas concedem permissões necessárias para casos de uso comuns, de maneira que você possa evitar a necessidade de investigar quais permissões são necessárias. Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSControlTowerAccountServiceRolePolicy— Uma nova política | O AWS Control Tower adicionou uma nova função vinculada ao serviço que permite que a AWS Control Tower crie e gerencie regras de eventos e, com base nessas regras, gerencie a detecção de desvios para controles relacionados ao Security Hub.<br><br>Essa mudança é necessária para que os clientes possam visualizar recursos dispersos no console, quando esses recursos estão relacionados aos controles do Security Hub que fazem parte do padrão gerenciado por serviços do Security Hub: AWS Control Tower. | 22 de maio de 2023 |
| AWS ControlTowerServiceRolePolicy: atualização para uma política existente | A AWS Control Tower adicionou novas permissões que permitem que a AWS Control Tower faça chamadas para`EnableReg` | 6 de abril de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | `ion` ,`ListRegions` , e `GetRegionOptStatus` APIs implementadas pelo serviço de gerenciamento de AWS contas, para Regiões da AWS disponibilizar o opt-in para contas de clientes na landing zone (conta de gerenciamento, conta de arquivamento de registros, conta de auditoria, contas de membros da OU).<br><br>Essa mudança é necessária para que os clientes tenham a opção de expandir a governança regional do AWS Control Tower para as regiões optativas. | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWS ControlTowerServiceRolePolicy: atualização para uma política existente | A AWS Control Tower adicionou novas permissões que permitem que a AWS Control Tower assuma a `AWSControlTowerBlueprintAccess` função na conta blueprint (hub), que é uma conta dedicada em uma organização, contendo esquemas predefinidos armazenados em um ou mais produtos do Service Catalog. O AWS Control Tower assume a `AWSControlTowerBlueprintAccess` função de realizar três tarefas: criar um portfólio do Service Catalog, adicionar o produto modelo solicitado e compartilhar o portfólio com uma conta membro solicitada no momento do provisionamento da conta.<br><br>Essa alteração é necessária para que os clientes possam provisionar contas personalizadas por meio do AWS Control Tower Account Factory. | 28 de outubro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWS ControlTowerServiceRolePolicy: atualização para uma política existente | O AWS Control Tower adicionou novas permissões que permitem aos clientes configurar AWS CloudTrail trilhas em nível organizacional, começando na versão 3.0 do landing zone.<br><br>O CloudTrail recurso baseado na organização exige que os clientes tenham acesso confiável habilitado para o CloudTrail serviço, e o usuário ou função do IAM deve ter permissão para criar uma trilha em nível organizacional na conta de gerenciamento. | 20 de junho de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWS ControlTowerServiceRolePolicy: atualização para uma política existente | O AWS Control Tower adicionou novas permissões que permitem que os clientes usem a criptografia de chaves do KMS.<br><br>O recurso KMS permite que os clientes forneçam sua própria chave KMS para criptografar seus registros. CloudTrail Os clientes também podem alterar a chave KMS durante a atualização ou reparo da landing zone. Ao atualizar a chave KMS, AWS CloudFormation precisa de permissões para chamar a AWS CloudTrail `PutEventSelector` API. A mudança na política é permitir que a AWS ControlTowerAdminfunção chame a AWS CloudTrail `PutEventSelector` API. | 28 de julho de 2021 |
| O AWS Control Tower começou a monitorar as mudanças | O AWS Control Tower começou a monitorar as mudanças em suas políticas AWS gerenciadas. | 27 de maio de 2021 |

# Segurança na AWS Control Tower

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. A eficácia da nossa segurança é regularmente testada e verificada por auditores de terceiros como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Control Tower, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelos AWS serviços que você usa. Você também é responsável por outros fatores, inclusive a confidencialidade dos dados, os requisitos da organização, as leis e as regulamentações vigentes.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Control Tower. Os tópicos a seguir mostram como configurar o AWS Control Tower para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos da AWS Control Tower.

## Proteção de dados na AWS Control Tower

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados na AWS Control Tower. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o AWS Control Tower ou outro Serviços da AWS usando o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

> **Note**
>
> O registro de atividades do usuário com AWS CloudTrail é feito automaticamente no AWS Control Tower quando você configura sua landing zone.

Para obter mais informações sobre proteção de dados, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança. AWSO Control Tower fornece as seguintes opções que você pode usar para ajudar a proteger o conteúdo que existe na sua landing zone:

Tópicos



## Criptografia em repouso

AWSO Control Tower usa buckets Amazon S3 e bancos de dados Amazon DynamoDB que são criptografados em repouso usando Amazon S3-Managed Keys (-S3) em apoio à sua landing zone. SSE Essa criptografia é configurada por padrão quando você configura sua landing zone. Opcionalmente, você pode configurar seu landing zone para criptografar recursos com KMS chaves de criptografia. Você também pode estabelecer criptografia em repouso para os serviços que você usa em sua landing zone para os serviços que a suportam. Para obter mais informações, consulte o capítulo de segurança da documentação on-line desse serviço.

## Criptografia em trânsito

AWSO Control Tower usa Transport Layer Security (TLS) e criptografia do lado do cliente para criptografia em trânsito em apoio à sua landing zone. Além disso, acessar o AWS Control Tower requer o uso do console, que só pode ser acessado por meio de um HTTPS endpoint. Essa criptografia é configurada por padrão quando você configura sua landing zone.

## Restringir o acesso ao conteúdo

Como uma melhor prática, você deve restringir o acesso ao subconjunto de usuários apropriado. Com o AWS Control Tower, você pode fazer isso garantindo que seus administradores de nuvem central e usuários finais tenham as IAM permissões corretas ou, no caso de usuários do IAM Identity Center, que estejam nos grupos corretos.

- Para obter mais informações sobre funções e políticas para IAM entidades, consulte o Guia IAM do usuário.

- Para obter mais informações sobre os grupos do IAM Identity Center que são criados quando você configura sua landing zone, consulteGrupos do IAM Identity Center para o AWS Control Tower.

# Validação de conformidade para AWS Control Tower

AWSO Control Tower é um serviço bem arquitetado que pode ajudar sua organização a atender às suas necessidades de conformidade com controles e melhores práticas. Além disso, auditores terceirizados avaliam a segurança e a conformidade de vários serviços que você pode usar em sua landing zone como parte de vários programas de AWS conformidade. Isso incluiSOC, PCI RAMPHIPAA, Fed e outros.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Serviços no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios no AWS Artifact no Guia do AWS Artifact usuário.

Sua responsabilidade de conformidade ao usar o AWS Control Tower é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em. AWS
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos compatíveis.
- AWS Recursos de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Config— Esse AWS serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

# Resiliência na AWS Control Tower

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade.

AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, que são conectadas por meio de redes de baixa latência, alto rendimento e altamente redundantes. As zonas de disponibilidade permitem projetar e operar aplicativos e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data centers tradicionais.

Para obter uma lista de Regiões da AWS onde o AWS Control Tower está disponível, consulteComo AWS as regiões funcionam com a AWS Control Tower.

Sua região de origem é definida como a AWS região na qual seu landing zone foi configurado.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

# Segurança de infraestrutura na AWS Control Tower

AWSA Control Tower é protegida pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa API chamadas AWS publicadas para acessar AWS serviços e recursos em sua landing zone por meio da rede. Exigimos o Transport Layer Security (TLS) 1.2 e recomendamos o Transport Layer Security (TLS) 1.3 ou posterior. Os clientes também devem oferecer suporte a pacotes de criptografia com sigilo direto perfeito (), como Ephemeral Diffie-Hellman (PFS) ou Elliptic Curve Ephemeral Diffie-Hellman (). DHE ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Você pode configurar grupos de segurança para fornecer segurança adicional de infraestrutura de rede para suas cargas de trabalho da zona de pouso da AWS Control Tower. Para obter mais informações, consulte Passo a passo: Configure grupos de segurança no AWS Control Tower com o AWS Firewall Manager.

# Registro e monitoramento na AWS Control Tower

O monitoramento permite planejar e responder a possíveis incidentes. Os resultados das atividades de monitoramento são armazenados em arquivos de log. Portanto, o registro e o monitoramento são conceitos intimamente relacionados e são uma parte importante da natureza bem arquitetada do AWS Control Tower.

Quando você configura sua landing zone, uma das contas compartilhadas criadas é a conta de arquivamento de registros. Ele se dedica a coletar todos os registros centralmente, incluindo registros de todas as suas contas compartilhadas e de membros. Os arquivos de log são armazenados em um bucket do Amazon S3. Esses arquivos de log permitem que administradores e auditores revisem as ações e os eventos ocorridos.

Como prática recomendada, você deve coletar dados de monitoramento de todas as partes da AWS configuração em seus registros, para poder depurar com mais facilidade uma falha de vários pontos, caso ocorra. AWS fornece várias ferramentas para monitorar seus recursos e atividades em sua landing zone.

Por exemplo, o status de seus controles é monitorado constantemente. Você pode ver seu status rapidamente no console do AWS Control Tower ou programaticamente por meio das APIs do AWS Control Tower. A integridade e o status das contas que você provisionou no Account Factory também são monitorados constantemente.

Exibir ações registradas na página Atividades

No console do AWS Control Tower, a página Atividades fornece uma visão geral das ações da conta de gerenciamento da AWS Control Tower. Para navegar até a página de atividades do AWS Control Tower, selecione Atividades no painel de navegação à esquerda.

As atividades mostradas na página Atividades são as mesmas relatadas no registro de AWS CloudTrail eventos do AWS Control Tower, mas são mostradas em formato de tabela. Para saber mais sobre uma atividade específica, selecione a atividade na tabela e escolha View details (Visualizar detalhes).

Você pode visualizar as ações e eventos da conta do membro nos arquivos de registro.

As seções a seguir descrevem o monitoramento e o registro no AWS Control Tower com mais detalhes:

Tópicos



# Sobre o login no AWS Control Tower

O AWS Control Tower realiza o registro automático de ações e eventos, por meio de sua integração com AWS CloudTrail e AWS Config, e os registra em. CloudWatch Todas as ações são registradas, incluindo ações da conta de gerenciamento do AWS Control Tower e das contas dos membros da sua organização. As ações e eventos da conta de gerenciamento podem ser visualizados na página Atividades no console. Você pode visualizar as ações e eventos da conta do membro nos arquivos de registro.

Trilhas em nível organizacional

O AWS Control Tower configura uma nova CloudTrail trilha quando você configura uma landing zone. É uma trilha no nível da organização, o que significa que ela registra todos os eventos da conta de gerenciamento e de todas as contas dos membros da organização. Esse recurso depende de acesso confiável para dar à conta de gerenciamento permissões para criar uma trilha em cada conta de membro.

Para obter mais informações sobre o AWS Control Tower e as trilhas CloudTrail da organização, consulte Como criar uma trilha para uma organização.

> **Note**
>
> Nas versões do AWS Control Tower antes da versão 3.0 do landing zone, a AWS Control Tower criou uma trilha de conta de membro em cada conta. Quando você atualiza para a versão 3.0, sua CloudTrail trilha se torna uma trilha organizacional. Para obter as melhores práticas ao se deslocar entre trilhas, consulte Práticas recomendadas para mudar trilhas no Guia CloudTrail do usuário.

Quando você inscreve uma conta no AWS Control Tower, sua conta é governada pela AWS CloudTrail trilha da organização da AWS Control Tower. Se você já tiver uma implantação de uma

CloudTrail trilha nessa conta, poderá ver cobranças duplicadas, a menos que exclua a trilha existente da conta antes de inscrevê-la no AWS Control Tower.

> **Note**
>
> Quando você atualiza para a versão 3.0 da landing zone, o AWS Control Tower exclui as trilhas no nível da conta (que a AWS Control Tower criou) nas suas contas inscritas em seu nome. Seus arquivos de log existentes em nível de conta são preservados em seu bucket Amazon S3.

## Política de bucket do Amazon S3 na conta de auditoria

No AWS Control Tower, AWS os serviços têm acesso aos seus recursos somente quando a solicitação é originada da sua organização ou unidade organizacional (OU). Uma `aws:SourceOrgID` condição deve ser atendida para qualquer permissão de gravação.

Você pode usar a chave de `aws:SourceOrgID` condição e definir o valor do ID da sua organização no elemento de condição da sua política de bucket do Amazon S3. Essa condição garante que CloudTrail somente registros em nome de contas dentro de sua organização possam ser gravados em seu bucket do S3; ela impede que CloudTrail registros de fora da sua organização gravem em seu bucket S3 do AWS Control Tower.

Essa política não afeta a funcionalidade de suas cargas de trabalho existentes. A política é mostrada no exemplo a seguir.

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
```

```
            Bool:
              aws:SecureTransport: false
        - Sid: AWSBucketPermissionsCheck
          Effect: Allow
          Principal:
            Service:
              - cloudtrail.amazonaws.com
              - config.amazonaws.com
          Action: s3:GetBucketAcl
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
        - Sid: AWSConfigBucketExistenceCheck
          Effect: Allow
          Principal:
            Service:
              - cloudtrail.amazonaws.com
              - config.amazonaws.com
          Action: s3:ListBucket
          Resource:
            - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
        - Sid: AWSBucketDeliveryForConfig
          Effect: Allow
          Principal:
            Service:
              - config.amazonaws.com
          Action: s3:PutObject
          Resource:
            - Fn::Join:
                - ""
                -
                  - !Sub "arn:${AWS::Partition}:s3:::"
                  - !Ref "S3AuditBucket"
                  - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
          Condition:
            StringEquals:
              aws:SourceOrgID: !Ref OrganizationId
        - Sid: AWSBucketDeliveryForOrganizationTrail
          Effect: Allow
          Principal:
            Service:
              - cloudtrail.amazonaws.com
          Action: s3:PutObject
          Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
```

```
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
            aws:SourceOrgID: !Ref OrganizationId
```

Para obter mais informações sobre essa chave de condição, consulte a documentação do IAM e a postagem no blog do IAM intitulada “Use controles escaláveis para AWS serviços que acessam seus recursos”.

## Ferramentas integradas para monitoramento

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS Control Tower e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar o AWS Control Tower, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- A Amazon CloudWatch Events fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. CloudWatch Os eventos permitem a computação automatizada baseada em eventos, pois você pode criar regras que observam determinados eventos e acionam ações automatizadas em outros AWS serviços quando esses eventos acontecem. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Events.
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.

- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram.

Dica: você pode ver e consultar a CloudTrail atividade em uma conta por meio do CloudWatch Logs e do CloudWatch Logs Insights. Essa atividade inclui eventos do ciclo de vida do AWS Control Tower. CloudWatchOs recursos dos registros permitem que você realize consultas mais granulares e precisas do que você normalmente seria capaz de fazer usando. CloudTrail

Para ter mais informações, consulte Registrando ações do AWS Control Tower com AWS CloudTrail.

# Registrando ações do AWS Control Tower com AWS CloudTrail

O AWS Control Tower é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço na AWS Control Tower. CloudTrail captura ações para o AWS Control Tower como eventos. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o AWS Control Tower.

Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao AWS Control Tower, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, inclusive como configurá-lo e ativá-lo, consulte o Guia AWS CloudTrail do usuário.

## Informações do AWS Control Tower em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre no AWS Control Tower, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

> **Note**
>
> Nas versões do AWS Control Tower antes da versão 3.0 do landing zone, a AWS Control Tower criou uma trilha de conta de membro. Quando você atualiza para a versão 3.0, sua CloudTrail trilha é atualizada para se tornar uma trilha da organização. Para obter as melhores práticas ao se mover entre trilhas, consulte Criação de uma trilha organizacional no Guia CloudTrail do usuário.

Recomendado: Crie uma trilha

Para um registro contínuo de eventos em sua AWS conta, incluindo eventos para o AWS Control Tower, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, ao criar uma trilha no console, ela é aplicada a todas as regiões da AWS . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão Geral para Criar uma Trilha
- Prepare-se para criar uma trilha
- Gerenciando CloudTrail custos
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

O AWS Control Tower registra as seguintes ações como eventos em arquivos de CloudTrail log:

APIs públicas

- Para obter uma lista completa das APIs públicas da AWS Control Tower e detalhes sobre cada uma delas, consulte The AWS Control Tower API Reference. As chamadas para essas APIs públicas são registradas por. AWS CloudTrail

Outras APIs

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService
- GetAvailableUpdates

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.
- Se a solicitação foi rejeitada, pois o acesso foi negado ou processado com sucesso.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

## Exemplo: entradas do arquivo de log do AWS Control Tower

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os eventos não aparecem em nenhuma ordem específica nos arquivos de log.

O exemplo a seguir mostra uma entrada de CloudTrail registro que mostra a estrutura de uma entrada típica de arquivo de log para um evento do `SetupLandingZone` AWS Control Tower, incluindo um registro da identidade do usuário que iniciou a ação.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

# Monitore as mudanças de recursos com AWS Config

O AWS Control Tower habilita AWS Config todas as contas inscritas, para que possa monitorar a conformidade por meio de controles de detetive, registrar alterações de recursos e entregar registros de alterações de recursos à conta de arquivamento de registros.

Se sua versão do landing zone for anterior à 3.0: para suas contas inscritas, AWS Config registra todas as alterações nos recursos, para todas as regiões nas quais a conta opera. Cada alteração é modelada como um item de configuração (CI), que contém informações como o identificador do recurso, a região, a data em que cada alteração foi registrada e se a alteração está relacionada a um recurso conhecido ou a um recém-descoberto.

Se a versão da sua landing zone for 3.0 ou posterior: o AWS Control Tower limita a gravação de recursos globais, como usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM,

somente à sua região de origem. Cópias das alterações globais de recursos não são armazenadas em todas as regiões. Essa limitação do registro de recursos está em conformidade com as AWS Config melhores práticas. Uma lista completa dos recursos globais está disponível na AWS Config documentação.

- Para saber mais AWS Config, consulte Como AWS Config funciona.
- Para obter uma lista de recursos que AWS Config podem oferecer suporte, consulte Tipos de recursos compatíveis.
- Para saber como personalizar o rastreamento de recursos no ambiente da AWS Control Tower, consulte a postagem do blog intitulada Personalizar o rastreamento de AWS Config recursos na AWS Control Tower.

O AWS Control Tower configura um canal AWS Config de entrega em todas as contas inscritas. Por meio desse canal de entrega, ele registra todas as alterações registradas AWS Config na conta de arquivamento de registros, onde elas são armazenadas em uma pasta em um bucket do Amazon Simple Storage Service.

## Gerencie AWS Config custos no AWS Control Tower

Esta seção descreve como AWS Config registra e cobra as alterações nos recursos em suas contas do AWS Control Tower. Essas informações podem ajudar você a entender como gerenciar os custos associados AWS Configà utilização do AWS Control Tower. O AWS Control Tower não adiciona nenhum custo adicional.

> **Note**
>
> Se a versão da sua landing zone for 3.0 ou posterior: o AWS Control Tower limita a AWS Config gravação de recursos globais, como usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM, somente à sua região de origem. Portanto, algumas das informações desta seção podem não se aplicar à sua landing zone.

AWS Config foi projetado para registrar cada alteração em cada recurso, em cada região em que uma conta opera, como um item de configuração (CI). AWS Config cobra por cada item de configuração que ele gera.

Como AWS Config opera

AWS Config registra recursos em cada região, separadamente. Alguns recursos globais, como funções do IAM, são registrados uma vez por região. Por exemplo, se você criar uma nova função do IAM em uma conta cadastrada que opera em cinco regiões, AWS Config gera cinco ICs, um para cada região. Outros recursos globais, como zonas hospedadas do Route 53, são registrados somente uma vez em todas as regiões. Por exemplo, se você criar uma nova zona hospedada do Route 53 em uma conta inscrita, AWS Config gera um CI, independentemente de quantas regiões estejam selecionadas para essa conta. Para obter uma lista que ajuda você a distinguir esses tipos de recursos, consulteO mesmo recurso é registrado várias vezes.

> **Note**
>
> Quando o AWS Control Tower trabalha com AWS Config, uma região pode ser governada pela AWS Control Tower ou não governada, e AWS Config ainda registra as alterações se a conta operar nessa região.

AWS Config detecta dois tipos de relacionamentos em recursos

AWS Config faz uma distinção entre relações diretas e indiretas entre recursos. Se um recurso for retornado na chamada da API Describe de outro recurso, esses recursos serão registrados como uma relação direta. Quando você altera um recurso em um relacionamento direto com outro recurso, AWS Config não cria um IC para ambos os recursos.

Por exemplo, se você criar uma instância do Amazon EC2 e a API exigir que você crie uma interface de rede, AWS Config considere que a instância do Amazon EC2 tem uma relação direta com a interface de rede. Como resultado, AWS Config gera somente um CI.

AWS Config registra alterações separadas para relacionamentos de recursos que são relacionamentos indiretos. Por exemplo, AWS Config gera dois CIs se você criar um grupo de segurança e adicionar uma instância associada do Amazon EC2 que faz parte do grupo de segurança.

Para obter mais informações sobre relacionamentos diretos e indiretos, consulte O que é um relacionamento direto e indireto com relação a um recurso?

Você pode encontrar uma lista de relacionamentos de recursos na AWS Config documentação.

## Visualize os dados do AWS Config gravador nas contas inscritas

AWS Config é integrado CloudWatch para que você possa visualizar AWS Config ICs em um painel. Para obter mais informações, consulte a postagem do blog intitulada AWS Config suporta CloudWatch as métricas da Amazon.

Programaticamente, para visualizar AWS Config dados, você pode trabalhar com a AWS CLI ou utilizar outras ferramentas. AWS

### Consulte os dados do AWS Config gravador em um recurso específico

Você pode usar a AWS CLI para recuperar uma lista das alterações mais recentes de um recurso.

Comando de histórico de recursos:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

Para saber mais, consulte a documentação da API para `get-config-history`.

### Visualize AWS Config dados com a Amazon QuickSight

Você pode visualizar e consultar recursos registrados por AWS Config toda a organização. Para obter mais informações, consulte Visualização de AWS Config dados usando o Amazon Athena e a Amazon. QuickSight

## Solução de problemas AWS Config no AWS Control Tower

Esta seção fornece informações sobre alguns problemas que você pode encontrar ao usar o AWS Config AWS Control Tower.

### AWS Config Custos elevados

Se seu fluxo de trabalho incluir processos que criam, atualizam ou excluem recursos com frequência, ou se ele manipula recursos em grande número, esse fluxo de trabalho pode gerar um grande número de ICs. Se você executar esses processos em uma conta que não seja de produção, considere cancelar a inscrição da conta. Talvez seja necessário desativar o AWS Config gravador dessa conta manualmente.

> **Note**
>
> Depois de cancelar a inscrição da conta, o AWS Control Tower não pode aplicar controles de detetive nem registrar eventos da conta, como AWS Config atividades, para obter recursos nessa conta.

Para obter mais informações, consulte Não gerenciar uma conta inscrita. Para saber como desativar o AWS Config gravador, consulte Gerenciando o gravador de configuração.

### O mesmo recurso é registrado várias vezes

Verifique se o recurso é global. Para zonas de pouso do AWS Control Tower anteriores à versão 3.0, é AWS Config possível registrar determinados recursos globais uma vez para cada região em que AWS Config está operando. Por exemplo, se AWS Config estiver ativado em oito regiões, cada função será registrada oito vezes.

Os seguintes recursos são registrados uma vez para cada região em que AWS Config está operando:

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Outros recursos globais são registrados somente uma vez. Aqui estão alguns exemplos de recursos que são registrados uma vez:

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

### AWS Config não registrou um recurso

Certos recursos têm relações de dependência com outros recursos. Essas relações podem ser diretas ou indiretas. Você pode encontrar uma lista de relacionamentos indiretos obsoletos nas Perguntas frequentes. AWS Config

## Eventos de ciclo de vida no AWS Control Tower

Alguns eventos registrados pelo AWS Control Tower são eventos de ciclo de vida. O objetivo de um evento de ciclo de vida é marcar a conclusão de determinadas ações do AWS Control Tower que alteram o estado dos recursos. Os eventos de ciclo de vida se aplicam aos recursos que o AWS Control Tower cria ou gerencia, como unidades organizacionais (OUs), contas e controles.

Características dos eventos do ciclo de vida do AWS Control Tower

- Para cada evento de ciclo de vida, o log de eventos mostra se a ação de origem do Control Tower foi concluída com êxito ou falhou.
- AWS CloudTrail registra automaticamente cada evento do ciclo de vida como um evento de serviço não relacionado à API AWS . Para obter mais informações, consulte o Guia AWS CloudTrail do usuário.
- Cada evento de ciclo de vida também é entregue aos serviços Amazon e EventBridge Amazon CloudWatch Events.

Os eventos de ciclo de vida no AWS Control Tower oferecem dois benefícios principais:

- Como um evento de ciclo de vida registra a conclusão de uma ação do AWS Control Tower, você pode criar uma regra da Amazon EventBridge ou uma regra da Amazon CloudWatch Events que pode acionar as próximas etapas em seu fluxo de trabalho de automação, com base no estado do evento do ciclo de vida.
- Os logs fornecem detalhes adicionais para auxiliar os administradores e auditores na revisão de determinados tipos de atividade nas organizações.

### Como funcionam os eventos de ciclo de vida

O AWS Control Tower depende de vários serviços para implementar suas ações. Portanto, cada evento de ciclo de vida é registrado somente após uma série de ações ser concluída. Por exemplo, quando você habilita um controle em uma OU, o AWS Control Tower lança uma série de subetapas

que implementam a solicitação. O resultado final de toda a série de subetapas é registrado no log como o estado do evento de ciclo de vida.

- Se cada subetapa subjacente tiver sido concluída com êxito, o estado do evento de ciclo de vida será registrado como Succeeded (Bem-sucedido).
- Se qualquer uma das subetapas subjacentes não tiver sido concluída com êxito, o estado do evento de ciclo de vida será registrado como Failed (Falhou).

Cada evento do ciclo de vida inclui um timestamp registrado que mostra quando a ação do AWS Control Tower foi iniciada e outro timestamp mostrando quando o evento do ciclo de vida foi concluído, marcando o sucesso ou o fracasso.

Como exibir eventos de ciclo de vida no Control Tower

Você pode visualizar os eventos do ciclo de vida na página Atividades no painel do AWS Control Tower.

- Para navegar até a página Activities (Atividades), selecione Activities (Atividades) no painel de navegação esquerdo.
- Para obter mais detalhes sobre um evento específico, selecione-o e escolha o botão View details (Exibir detalhes) no canto superior direito.

Para obter mais informações sobre como integrar eventos do ciclo de vida do AWS Control Tower aos seus fluxos de trabalho, consulte esta postagem do blog, Usando eventos de ciclo de vida para rastrear ações do AWS Control Tower e acionar fluxos de trabalho automatizados.

Comportamento esperado CreateManagedAccount e eventos do UpdateManagedAccount ciclo de vida

Quando você cria uma conta ou inscreve uma conta no AWS Control Tower, essas duas ações chamam a mesma API interna. Se houver um erro durante o processo, ele geralmente ocorre após a criação da conta, mas não está totalmente provisionada. Quando você tenta criar a conta novamente após o erro ou ao tentar atualizar o produto provisionado, o AWS Control Tower vê que a conta já existe.

Como a conta existe, o AWS Control Tower registra o evento do `UpdateManagedAccount` ciclo de vida em vez do evento do `CreateManagedAccount` ciclo de vida no final da solicitação de nova tentativa. Talvez você esperasse ver outro `CreateManagedAccount` evento por causa do erro.

No entanto, o evento do `UpdateManagedAccount` ciclo de vida é o comportamento esperado e desejado.

Se você planeja criar ou inscrever contas no AWS Control Tower usando métodos automatizados, programe a função Lambda UpdateManagedAccountpara procurar eventos do ciclo de vida, bem como eventos do ciclo de vida. CreateManagedAccount

Nomes dos eventos de ciclo de vida

Cada evento do ciclo de vida é nomeado de forma que corresponda à ação originária do AWS Control Tower, que também é registrada pela AWS. CloudTrail Assim, por exemplo, um evento de ciclo de vida originado pelo evento AWS Control Tower `CreateManagedAccount` CloudTrail é nomeado. `CreateManagedAccount`

Cada nome na lista a seguir é um link para um exemplo do detalhamento registrado em log no formato `JSON`. Os detalhes adicionais mostrados nesses exemplos foram retirados dos registros de CloudWatch eventos da Amazon.

Embora o `JSON` não ofereça suporte a comentários, alguns comentários foram acrescentados nos exemplos para fins explicativos. Eles são precedidos por "//" e aparecem no lado direito dos exemplos.

Nesses exemplos, alguns nomes de conta e de organização foram obscurecidos. Um `accountId` é sempre uma sequência de 12 números, substituída por "xxxxxxxxxxxx" nos exemplos. Um `organizationalUnitID` é uma cadeia única de letras e números. A forma foi preservada nos exemplos.

- `CreateManagedAccount`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para criar e provisionar uma nova conta usando a fábrica de contas.
- `UpdateManagedAccount`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para atualizar um produto provisionado associado a uma conta que você criou anteriormente usando a fábrica de contas.
- `EnableGuardrail`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para permitir o controle de uma OU criada pela AWS Control Tower.
- `DisableGuardrail`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para desativar um controle em uma OU criada pela AWS Control Tower.
- `SetupLandingZone`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para configurar uma landing zone.

- UpdateLandingZone: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para atualizar sua landing zone existente.
- RegisterOrganizationalUnit: O registro registra se o AWS Control Tower concluiu com sucesso todas as ações para habilitar seus recursos de governança em uma OU.
- DeregisterOrganizationalUnit: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para desativar seus recursos de governança em uma OU.
- PrecheckOrganizationalUnit: o registro registra se o AWS Control Tower detectou algum recurso que impediria a conclusão bem-sucedida da operação de governança do Extend.

As seções a seguir fornecem uma lista dos eventos do ciclo de vida do AWS Control Tower, com exemplos dos detalhes registrados para cada tipo de evento do ciclo de vida.

## CreateManagedAccount

Esse evento do ciclo de vida registra se o AWS Control Tower criou e provisionou com sucesso uma nova conta usando a fábrica de contas. Esse evento corresponde ao evento AWS Control Tower `CreateManagedAccount` CloudTrail . O log de eventos de ciclo de vida inclui o `accountName` e o `accountId` da conta recém-criada, e o `organizationalUnitName` e o `organizationalUnitId` da UO em que a conta foi colocada.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
```

```
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

## UpdateManagedAccount

Esse evento do ciclo de vida registra se o AWS Control Tower atualizou com sucesso o produto provisionado associado a uma conta que foi criada anteriormente usando a fábrica de contas. Esse evento corresponde ao evento AWS Control Tower `UpdateManagedAccount` CloudTrail. O log de eventos de ciclo de vida inclui o `accountName` e `accountId` da conta associada e o `organizationalUnitName` e `organizationalUnitId` da UO em que a conta atualizada é colocada.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
```

```
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

# EnableGuardrail

Esse evento do ciclo de vida registra se o AWS Control Tower habilitou com sucesso um controle em uma OU que está sendo gerenciada pela AWS Control Tower. Esse evento corresponde ao evento AWS Control Tower `EnableGuardrail` CloudTrail . O registro de eventos do ciclo de vida inclui a `guardrailId` extremidade `guardrailBehavior` do controle `organizationalUnitName` e a extremidade `organizationalUnitId` da OU na qual o controle está ativado.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                  // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                           // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
```

```
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```

## DisableGuardrail

Esse evento de ciclo de vida registra se o AWS Control Tower desativou com sucesso um controle em uma OU que está sendo gerenciada pela AWS Control Tower. Esse evento corresponde ao evento AWS Control Tower `DisableGuardrail` CloudTrail . O registro de eventos do ciclo de vida inclui a `guardrailId` `guardrailBehavior` extremidade do controle `organizationalUnitName` e a extremidade `organizationalUnitId` da OU na qual o controle está desativado.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
```

```
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
            }
        }
    }
```

## SetupLandingZone

Esse evento de ciclo de vida registra se o AWS Control Tower configurou com sucesso uma landing zone. Esse evento corresponde ao evento AWS Control Tower `SetupLandingZone` CloudTrail . O registro de eventos do ciclo de vida inclui `orootOrganizationalId`, que é o ID da organização que o AWS Control Tower cria a partir da conta de gerenciamento. A entrada de registro também inclui a `organizationalUnitName` e `organizationalUnitId` para cada uma das OUs e a `accountName` e `accountId` para cada conta, que são criadas quando o AWS Control Tower configura a landing zone.

```
{
    "version": "0",
```

```
   "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
   "detail-type": "AWS Service Event via CloudTrail",
   "source": "aws.controltower",
   "account": "XXXXXXXXXXXX",                                   // Management account
ID.
   "time": "2018-08-30T21:42:18Z",                              // Event time from
CloudTrail.
   "region": "us-east-1",                                       // Management account
CloudTrail region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                         // Management-account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "SetupLandingZone",
       "awsRegion": "us-east-1",                                // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                        // This value is
generated by CloudTrail.
       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "setupLandingZoneStatus": {
               "state": "SUCCEEDED",                             // Status of entire
lifecycle operation.
               "message": "AWS Control Tower successfully set up a new landing zone.",

               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                         // Use a list.
                 {
                   "organizationalUnitName": "Security",            // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",           // Custom OU name.
```

```
                    "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                  },
                ],
               "accounts": [                                      // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

## UpdateLandingZone

Esse evento de ciclo de vida registra se o AWS Control Tower atualizou com sucesso sua landing zone existente. Esse evento corresponde ao evento AWS Control Tower `UpdateLandingZone` CloudTrail . O registro de eventos do ciclo de vida inclui `orootOrganizationalId`, que é o ID da organização (atualizada) governada pela AWS Control Tower. A entrada de registro também inclui a `organizationalUnitName` e `organizationalUnitId` para cada uma das OUs e a `accountName` e `accountId` para cada conta, que foi criada anteriormente, quando o AWS Control Tower configurou originalmente a landing zone.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                 // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Event time from
 CloudTrail.
```

```
   "region": "us-east-1",                                          // Management account
CloudTrail region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                            // Management account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                        // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "UpdateLandingZone",
       "awsRegion": "us-east-1",                                   // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                           // This value is
generated by CloudTrail.

       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "updateLandingZoneStatus": {
               "state": "SUCCEEDED",                               // Status of entire
operation.
               "message": "AWS Control Tower successfully updated a landing zone.",


               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                           // Use a list.
                 {
                   "organizationalUnitName": "Security",             // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                 },
                 {
                   "organizationalUnitName": "Custom",             // Custom OU name.
                   "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                 },
               ],
              "accounts": [                                        // All created
accounts are here. Use a list of "account" objects.
```

```
                {
                  "accountName": "Audit",
                  "accountId": "XXXXXXXXXXXX"
                },
                {
                  "accountName": "Log archive",
                  "accountId": "XXXXXXXXXX"
                }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

## RegisterOrganizationalUnit

Esse evento de ciclo de vida registra se o AWS Control Tower habilitou com sucesso seus recursos de governança em uma OU. Esse evento corresponde ao evento AWS Control Tower `RegisterOrganizationalUnit` CloudTrail . O registro de eventos do ciclo de vida inclui o fim `organizationalUnitName` `organizationalUnitId` da OU que o AWS Control Tower colocou sob sua governança.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
```

```
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

## DeregisterOrganizationalUnit

Esse evento de ciclo de vida registra se o AWS Control Tower desativou com sucesso seus recursos de governança em uma OU. Esse evento corresponde ao evento AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail . O registro de eventos do ciclo de vida inclui a extremidade `organizationalUnitName` `organizationalUnitId` da OU na qual o AWS Control Tower desativou seus recursos de governança.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
```

```
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
organizational unit, and enabled mandatory guardrails on the new organizational
unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                   // Foundational
OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"          // Foundational
OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

## PrecheckOrganizationalUnit

Esse evento do ciclo de vida registra se o AWS Control Tower realizou com sucesso as pré-verificações em uma OU. Esse evento corresponde ao evento AWS Control Tower `PrecheckOrganizationalUnit` CloudTrail . O registro de eventos do ciclo de vida contém um

campo para os `failedPrechecks` valores`Id`,`Name`, e para cada recurso no qual o AWS Control Tower realizou pré-verificações durante o processo de registro da OU.

O registro de eventos também contém informações sobre as contas aninhadas nas quais as pré-verificações foram realizadas, incluindo os `accountName` campos`accountId`, e. `failedPrechecks`

Se o `failedPrechecks` valor estiver vazio, significa que todas as pré-verificações desse recurso foram aprovadas com êxito.

- Esse evento é emitido somente se houver uma falha na pré-verificação.
- Esse evento não será emitido se você estiver registrando uma OU vazia.

Exemplo de evento:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
```

```
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
}
```

# Usando notificações AWS de usuário com AWS Control Tower

Você pode usar as notificaçõesAWS do usuário para configurar canais de entrega para ser notificado sobre AWS Control Tower eventos. Você recebe uma notificação quando um evento corresponde

a uma regra especificada. Você pode receber notificações de eventos por meio de vários canais, incluindo e-mail, notificações de AWS Chatbotbate-papo ou notificações push AWS do Console Mobile App. Você também pode ver as notificações na Central de notificações do console.

AWS As notificações do usuário oferecem suporte à agregação, o que pode reduzir o número de notificações que você recebe durante eventos específicos. As notificações também estão visíveis na Central de Notificações do Console.

As vantagens de assinar notificações por meio de notificações de AWS usuário em vez de EventBridge incluem:

- Uma interface de usuário (UI) mais amigável.
- Integração com o AWS console, na área de campainha/notificações na barra de navegação global.
- Suporte nativo para notificações por e-mail, não há necessidade de configurar o Amazon SNS.
- Mais notavelmente, o suporte para notificações push móveis, exclusivo para notificações AWS do usuário.

Por exemplo, um tipo de notificação que você pode querer receber é no caso de descobertas críticas e de alta gravidade do Security Hub. Um trecho de código em JSON para configurar essa assinatura de notificação pode ter a seguinte aparência:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Filtragem de eventos

- Você pode filtrar eventos por serviço e nome usando os filtros disponíveis no console de notificações AWS do usuário.
- Você pode filtrar eventos por propriedades específicas se criar seu próprio EventBridge filtro a partir do código JSON.

### Exemplo de AWS Control Tower evento

Aqui está um exemplo de evento generalizado para AWS Control Tower.

- É um EventBridge evento.
- Você pode se inscrever em EventBridge eventos (como este) usando as Notificações AWS do Usuário.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
```

```
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

# Instruções

Este capítulo contém procedimentos passo a passo que podem ajudá-lo a usar o AWS Control Tower.

Tópicos



## Passo a passo: mude do ALZ para o AWS Control Tower

Muitos AWS clientes adotaram a solução AWS Landing Zone (ALZ) para configurar um ambiente seguro, compatível e com várias AWS contas. Para reduzir a carga de gerenciar uma landing zone, AWS criei o serviço gerenciado chamado AWS Control Tower.

Nenhum recurso adicional está programado para o ALZ; ele está disponível apenas para suporte de longo prazo. Portanto, recomendamos que você mude da ALZ para o serviço AWS Control Tower. O blog vinculado a este capítulo explica diferentes considerações sobre essa mudança e explica como você pode planejar uma migração bem-sucedida do ALZ para o AWS Control Tower.

Blog: Migre a solução AWS Landing Zone para o AWS Control Tower

AWS A orientação prescritiva oferece uma documentação mais extensa, incluindo etapas para a transição do ALZ para o AWS Control Tower. Basicamente, você habilitará a governança do AWS Control Tower em sua organização atual que está executando o ALZ, com base em vários pré-requisitos. Para obter informações, consulte Transição da zona de AWS pouso para o AWS Control Tower.

# Passo a passo: Automatize o provisionamento de contas no AWS Control Tower por meio das APIs do Service Catalog

O AWS Control Tower é integrado a vários outros AWS serviços, como AWS Service Catalog. Você pode usar as APIs para criar e provisionar suas contas de membros no AWS Control Tower.

O vídeo mostra como provisionar contas de forma automatizada e em lote, chamando as AWS Service Catalog APIs. Para provisionamento, você chamará a `ProvisionProduct`API a partir da interface de linha de AWS comando (CLI) e especificará um arquivo JSON que contém os parâmetros de cada conta que você gostaria de configurar. O vídeo ilustra a instalação e o uso doAWS ambiente de desenvolvimento Cloud9 para realizar esse trabalho. Os comandos da CLI seriam os mesmos se você usasse o Cloudshell AWS em vez do Cloud9. AWS

> **Note**
>
> Você também pode adaptar essa abordagem para automatizar as atualizações da conta, chamando a `UpdateProvisionedProduct`API de AWS Service Catalog para cada conta. Você pode escrever um script para atualizar as contas, uma por uma.

Como um método de automação completamente diferente, se você estiver familiarizado com o Terraform, poderá provisionar contas com o AWS Control Tower Account Factory for Terraform (AFT).

Exemplo de função de administração de automação

Aqui está um exemplo de modelo que você pode usar para ajudar a configurar sua função de administração de automação na conta de gerenciamento. Você configuraria essa função em sua conta de gerenciamento para que ela pudesse realizar a automação com acesso de administrador nas contas de destino.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
```

```
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Exemplo de função de execução de automação

Aqui está um modelo de exemplo que você pode usar para ajudar a configurar a função de execução de automação. Você configuraria essa função nas contas de destino.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
```

```
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Depois de configurar essas funções, você chama as AWS Service Catalog APIs para realizar as tarefas automatizadas. Os comandos da CLI são fornecidos no vídeo.

## Exemplo de entrada de provisionamento para a API Service Catalog

Aqui está um exemplo da entrada que você pode fornecer à API do Service Catalog se estiver usando a `ProvisionProduct` API para provisionar contas do AWS Control Tower:

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
```

```
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

Para obter mais informações, consulte a referência da API do Service Catalog.

> **Note**
>
> Observe que o formato da string de entrada para o valor de `ManagedOrganizationalUnit` foi alterado de `OU_NAME` para`OU_NAME (OU_ID)`. O vídeo a seguir não menciona essa mudança.

## Passo a passo em vídeo

Este vídeo (6:58) descreve como automatizar implantações de contas no AWS Control Tower. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Vídeo passo a passo do provisionamento automatizado de contas no AWS Control Tower.

# Passo a passo: Configurar o AWS Control Tower sem uma VPC

Este tópico explica como configurar suas contas do AWS Control Tower sem uma VPC.

Se sua carga de trabalho não exigir uma VPC, poderá fazer o seguinte:

- Você pode excluir a nuvem privada virtual (VPC) do AWS Control Tower. Essa VPC foi criada ao configurar sua zona de destino.
- Você pode alterar as configurações do Account Factory para que novas contas do AWS Control Tower sejam criadas sem uma VPC associada.

> **Important**
>
> Se você provisionar contas do Account Factory com as configurações de acesso à Internet da VPC ativadas, essa configuração da Account Factory substituirá o controle Proibir o acesso à Internet para uma instância da Amazon VPC gerenciada por um cliente. Para evitar a ativação do acesso à Internet para contas recém-provisionadas, você deve alterar a configuração no Account Factory.

## Exclua a VPC do AWS Control Tower

Fora da AWS Control Tower, cada AWS cliente tem uma VPC padrão, que você pode ver no console da Amazon Virtual Private Cloud (Amazon VPC) em https://console.aws.amazon.com/vpc/. Você reconhecerá a VPC padrão, pois seu nome sempre inclui a palavra (default) no final do nome.

Quando você configura uma landing zone da AWS Control Tower, a AWS Control Tower exclui sua VPC AWS padrão e cria uma nova VPC padrão da AWS Control Tower. A nova VPC está associada à sua conta de gerenciamento do AWS Control Tower. Este tópico se refere a essa nova VPC como Control Tower VPC.

Ao visualizar sua VPC do AWS Control Tower no console da Amazon VPC, você não verá a palavra (padrão) no final do nome. Se você tiver mais de uma VPC, deverá usar o intervalo CIDR atribuído para identificar a VPC correta do AWS Control Tower.

Você pode excluir a VPC da AWS Control Tower, mas se posteriormente precisar de uma VPC na AWS Control Tower, você mesmo deverá criá-la.

Para excluir a VPC do AWS Control Tower

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Pesquise **VPC** ou selecione VPC nas opções do Service Catalog. Será exibido o VPC Dashboard (Painel da VPC).
3. No menu à esquerda, escolha Your VPCs (Suas VPCs). Será exibida uma lista de todas as suas VPCs.
4. Identifique a VPC do AWS Control Tower por sua faixa de CIDR.
5. Para excluir a VPC, escolha Actions (Ações) e Delete VPC (Excluir VPC).

Já existe uma VPC AWS (padrão) em todas as regiões da conta de gerenciamento do AWS Control Tower. Para seguir as melhores práticas de segurança, se você optar por excluir a VPC do AWS Control Tower, é melhor também excluir a AWS VPC padrão associada à conta de gerenciamento de todas as regiões. AWS Portanto, para proteger a conta de gerenciamento, remova a VPC padrão de cada região, bem como a VPC criada pela Control Tower na sua região de origem do AWS Control Tower.

## Crie uma conta no AWS Control Tower sem uma VPC

Se suas cargas de trabalho de usuário final não precisarem de VPCs, você poderá usar esse método para configurar contas de usuário final que não tenham VPCs criadas automaticamente para elas.

No painel do AWS Control Tower, você pode visualizar e editar suas configurações de rede. Depois de alterar as configurações para que as contas do AWS Control Tower sejam criadas sem uma VPC associada, todas as novas contas são criadas sem uma VPC até que você altere as configurações novamente.

Para configurar o Account Factory para criar contas sem VPCs

1. Abra um navegador da web e navegue até o console do AWS Control Tower em https://console.aws.amazon.com/controltower.
2. Escolha Account Factory no menu à esquerda.
3. Em seguida, você verá a página Account Factory com a seção Configuração de rede.
4. Observe as configurações atuais caso pretenda restaurá-las posteriormente.
5. Escolha o botão Edit (Editar) na seção Network Configuration (Configuração de rede).

6. Na página Edit account factory network configuration (Editar configuração de rede de fábrica da conta), acesse a seção VPC Configuration options for new accounts (Opções de configuração da VPC para novas contas).

   Você pode seguir a Opção 1 ou a Opção 2, ou ambas, para garantir que o AWS Control Tower não crie uma VPC ao provisionar uma conta.

   a. Opção 1 — Removendo sub-redes

      - Desative o botão de alternância Internet-accessible subnet (Sub-rede acessível pela Internet).
      - Defina o valor Maximum number of private subnets (Número máximo de sub-redes privadas) como 0.

   b. Opção 2 — Remoção de AWS regiões

      - Desmarque todas as caixas de seleção na coluna Regions for VPC creation (Regiões para criação de VPC).

7. Escolha Salvar.

### Possíveis erros

Esteja ciente desses possíveis erros que podem ocorrer quando você exclui sua VPC do AWS Control Tower ou reconfigura o Account Factory para criar contas sem VPCs.

- Sua conta de gerenciamento existente pode ter dependências ou recursos na VPC da AWS Control Tower, o que pode causar um erro de falha de exclusão.
- Se você deixar o CIDR padrão em vigor ao configurar para iniciar novas contas sem uma VPC, sua solicitação falhará com um erro informando que o CIDR não é válido.

## Passo a passo: Configure grupos de segurança no AWS Control Tower com o AWS Firewall Manager

O vídeo mostra como usar o serviço AWS Firewall Manager para oferecer melhorias na segurança da sua rede para o AWS Control Tower. Você pode designar uma conta de administrador de segurança que esteja habilitada para configurar grupos de segurança. Você verá como você pode configurar políticas de segurança e aplicar regras de segurança para suas organizações do

AWS Control Tower e como você pode remediar recursos não compatíveis aplicando políticas automaticamente. Você pode visualizar os grupos de segurança que estão em vigor para cada conta e recurso (como uma instância do Amazon EC2) em sua organização.

Você pode criar as suas próprias políticas de firewall ou assinar regras de fornecedores confiáveis.

### Configurar grupos de segurança com o AWS Firewall Manager

Este vídeo (8:02) descreve como configurar uma melhor segurança da infraestrutura de rede para seus recursos e cargas de trabalho no AWS Control Tower. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Passo a passo em vídeo da configuração do firewall no AWS Control Tower.

Para obter mais informações, consulte a documentação sobre como configurar o AWS WAF.

## Passo a passo: Descomissione uma zona de pouso do AWS Control Tower

O AWS Control Tower permite que você configure e administre AWS ambientes seguros de várias contas, conhecidos como zonas de pouso. O processo de limpeza de todos os recursos alocados pela AWS Control Tower é chamado de descomissionamento de uma landing zone.

Se você não quiser mais usar o AWS Control Tower, a ferramenta de descomissionamento automatizado limpa os recursos alocados pela AWS Control Tower. Para iniciar o processo de descomissionamento automatizado, navegue até a página Configurações da zona de pouso, selecione a guia de desativação e escolha Descomissionar zona de pouso.

Para obter uma lista das ações realizadas durante o descomissionamento, consulte. Visão geral do processo de descomissionamento

> **Warning**
>
> Excluir manualmente todos os seus recursos do AWS Control Tower não é o mesmo que descomissionar. Isso não permitirá que você configure uma nova landing zone.

Seus dados e os existentes não AWS Organizations são alterados pelo processo de descomissionamento, das seguintes maneiras.

- O AWS Control Tower não remove seus dados, apenas partes da zona de destino que é criada.
- Após a conclusão do processo de desativação, alguns artefatos de recursos permanecem, como buckets do Amazon S3 e grupos de log do Amazon Logs. CloudWatch Esses recursos devem ser excluídos manualmente antes da configuração de outra zona de destino para evitar possíveis custos associados à manutenção de determinados recursos.
- Você não pode usar a desativação automatizada para remover uma zona de destino parcialmente configurada. Se ocorrer uma falha no processo de configuração da zona de destino, você poderá resolver o estado de falha e configurá-lo até o fim para tornar possível a desativação automatizada ou será necessário excluir os recursos individualmente de forma manual.

A desativação de uma zona de destino é um processo de consequências significativas e não pode ser desfeito. As ações de descomissionamento tomadas pelo AWS Control Tower e os artefatos que permanecem após o descomissionamento estão descritos nas seções a seguir.

> **Important**
>
> Recomendamos veementemente a realização deste processo de desativação exclusivamente se você pretende parar de usar a zona de destino. Não é possível recriar uma zona de destino existente depois de sua desativação.

## Visão geral do processo de descomissionamento

Quando você solicita o descomissionamento da sua landing zone, o AWS Control Tower executa as seguintes ações.

- Desativa cada controle de detetive ativado na landing zone. O AWS Control Tower exclui os AWS CloudFormation recursos que dão suporte ao controle.
- Desativa cada controle preventivo removendo as políticas de controle de serviço (SCPs) do. AWS Organizations Se uma política estiver vazia (o que deveria acontecer após a remoção de todas as SCPs gerenciadas pela AWS Control Tower), a AWS Control Tower desanexará e excluirá totalmente a política.
- Exclui todos os blueprints implantados como. AWS CloudFormation StackSets
- Exclui todos os blueprints implantados como CloudFormation pilhas em todas as regiões.
- Para cada conta provisionada, o AWS Control Tower executa as seguintes ações durante o processo de descomissionamento.

  - Exclui os registros de cada conta de fábrica de contas.
  - Revoga as permissões da AWS Control Tower para a conta removendo a função do IAM que a AWS Control Tower criou (a menos que políticas adicionais tenham sido adicionadas a ela) e recria a `OrganizationsFullAccessRole` função padrão do IAM.
  - Remove os registros da conta de AWS Service Catalog.
  - Remove o produto e o portfólio da fábrica de contas do AWS Service Catalog.
- Exclui os esquemas das contas compartilhadas (Auditoria e Arquivo de Registros).
- Revoga as permissões da AWS Control Tower das contas compartilhadas removendo a função do IAM criada pela AWS Control Tower (a menos que políticas adicionais tenham sido adicionadas a ela) e recria a `OrganizationsFullAccessRole` função do IAM.
- Exclui registros relacionados às contas compartilhadas.
- Exclui registros relacionados a UOs criadas pelo cliente.
- Exclui registros internos que identificam a região de origem.

> **Note**
>
> Após a desativação, será possível remover o esquema da VPC da Fábrica de contas (`BP_ACCOUNT_FACTORY_VPC`) para limpar as rotas e gateways NAT, se sua VPC não estiver vazia.

## Recursos não removidos durante o descomissionamento

O descomissionamento de uma landing zone não reverte totalmente o processo de configuração do AWS Control Tower. Alguns recursos permanecem, os quais podem ser removidos manualmente.

AWS Organizations

Para clientes sem AWS Organizations organizações existentes, o AWS Control Tower configura uma organização com duas unidades organizacionais (OUs), chamadas Security e Sandbox. Ao desativar a zona de destino, a hierarquia da organização é preservada, da seguinte forma:

- As unidades organizacionais (OUs) que você criou no console do AWS Control Tower não são removidas.
- As OUs de segurança e sandbox não são removidas.

- A organização não foi excluída do AWS Organizations.
- Nenhuma conta AWS Organizations (compartilhada, provisionada ou gerenciada) é movida ou removida.

### AWS IAM Identity Center (SSO)

Para clientes sem um diretório existente do IAM Identity Center, o AWS Control Tower configura o IAM Identity Center e configura um diretório inicial. Quando você descomissiona sua landing zone, o AWS Control Tower não faz alterações no IAM Identity Center. Se necessário, você pode excluir manualmente as informações do IAM Identity Center armazenadas na sua conta de gerenciamento. Estas áreas, especificamente, permanecem inalteradas com a desativação:

- Os usuários criados com a fábrica de contas não são removidos.
- Os grupos criados pela configuração do AWS Control Tower não são removidos.
- Os conjuntos de permissões criados pelo AWS Control Tower não são removidos.
- As associações entre contas da AWS e conjuntos de permissões do IAM Identity Center não são removidas.
- Os diretórios do IAM Identity Center não são alterados.

### Funções

Durante a configuração, o AWS Control Tower cria determinadas funções para você se você usa o console, ou solicita que você crie essas funções se você configurar sua landing zone por meio das APIs. Quando você desativa sua landing zone, as seguintes funções não são removidas:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

### Buckets do Amazon S3

Durante a configuração, o AWS Control Tower cria buckets na conta de registro para registro e acesso ao registro. Ao desativar a zona de destino, os seguintes recursos não são removidos:

- O registro em log e o acesso de registro dos buckets do S3 na conta de registro não são removidos.
- O conteúdo dos buckets de acesso de registro e registro em log não é removido.

### Contas compartilhadas

Duas contas compartilhadas (Audit e Log Archive) são criadas na OU de segurança durante a configuração do AWS Control Tower. Ao desativar a zona de destino:

- As contas compartilhadas que foram criadas durante a configuração do AWS Control Tower não são fechadas.
- A função `OrganizationAccountAccessRole` do IAM é recriada para se alinhar à configuração padrão AWS Organizations .
- A função `AWSControlTowerExecution` é removida.

### Contas provisionadas

Os clientes do AWS Control Tower podem usar a fábrica de contas para criar novas contas da AWS. Ao desativar a zona de destino:

- As contas provisionadas criadas com a Fábrica de contas não são encerradas.
- Os produtos provisionados não AWS Service Catalog são removidos. Se você os limpar encerrando, suas contas serão movidas para a OU raiz.
- A VPC criada pelo AWS Control Tower não é removida e o conjunto de AWS CloudFormation pilhas associado (`BP_ACCOUNT_FACTORY_VPC`) não é removido.
- A função `OrganizationAccountAccessRole` do IAM é recriada para se alinhar à configuração padrão AWS Organizations .
- A função `AWSControlTowerExecution` é removida.

### CloudWatch Grupo de registros

Um grupo de CloudWatch registros de registros`aws-controltower/CloudTrailLogs`,, é criado como parte do blueprint chamado`AWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT`. Esse grupo de logs não é removido. Em vez disso, o esquema é excluído e os recursos são mantidos.

- Esse grupo de logs deve ser excluído manualmente antes da configuração de outra zona de destino.

> **Note**
>
> Os clientes na landing zone 3.0 e versões posteriores não precisam excluir os registros e CloudTrail as funções de CloudTrail registros de suas contas individuais inscritas, pois eles são criados somente na conta de gerenciamento, para a trilha em nível organizacional.
> A partir da versão 3.2 do landing zone, o AWS Control Tower cria uma EventBridge regra da Amazon, chamada`AWSControlTowerManagedRule`. Essa regra é criada em cada conta de membro, para todas as regiões governadas. A regra não é excluída automaticamente durante o descomissionamento, então você deve excluí-la manualmente das contas compartilhadas e membros de todas as regiões governadas antes de poder configurar uma landing zone em uma nova região.

Os procedimentos sobre como excluir recursos do AWS Control Tower são fornecidos emGerencie os recursos do AWS Control Tower.

## Gerencie os recursos do AWS Control Tower

Este documento fornece instruções sobre como remover recursos do AWS Control Tower individualmente, como parte de tarefas administrativas e de manutenção regulares. Os procedimentos fornecidos neste capítulo destinam-se somente à remoção de recursos individuais, ou de alguns recursos, quando necessário. Não é o mesmo que descomissionar sua landing zone.

Dois tipos de tarefas podem exigir a remoção de recursos:

- Para excluir recursos enquanto você gerencia sua zona de destino em situações comuns.
- Para limpar os recursos que permanecem após o descomissionamento automático.

> **Warning**
>
> A remoção manual de recursos não permitirá que você configure uma nova landing zone. Não é o mesmo que descomissionamento. Se você pretende descomissionar sua zona de pouso do AWS Control Tower, siga as instruções Passo a passo: Descomissione uma zona de pouso do AWS Control Tower antes de realizar qualquer ação descrita neste capítulo. As

instruções neste capítulo podem ajudá-lo a limpar os recursos que restam após a conclusão do descomissionamento automático. Mesmo que você exclua todos os recursos da sua zona de pouso manualmente, isso não é o mesmo que descomissionar a zona de pouso, e você poderá incorrer em cobranças inesperadas.

Se você precisar remover uma conta do AWS Control Tower, consulte as seções a seguir para fechar uma conta:

- Desgerenciar uma conta
- Fechar uma conta criada no Account Factory

Preciso descomissionar em vez de excluir?

Se você não pretende mais usar o AWS Control Tower para sua empresa ou se precisar de uma grande reimplantação de seus recursos organizacionais, talvez queira desativar os recursos criados quando você configurou inicialmente sua landing zone.

- Após a conclusão do processo de desativação, alguns artefatos de recursos permanecem, como buckets do Amazon S3 e grupos de log do Amazon Logs. CloudWatch
- Você deve limpar os recursos restantes em suas contas manualmente antes de configurar outra landing zone e evitar a possibilidade de cobranças inesperadas. Para ter mais informações, consulte Recursos não removidos durante o descomissionamento.

⚠ Warning

É altamente recomendável que você execute um processo de descomissionamento somente se pretender parar de usar seu landing zone. Esse processo não pode ser desfeito.

Sobre a remoção de recursos do AWS Control Tower

Os procedimentos individuais deste capítulo orientam você pelos métodos manuais de remoção de recursos do AWS Control Tower. Esses procedimentos podem ser seguidos quando você precisar excluir um recurso específico da sua landing zone.

Antes de realizar esses procedimentos, a menos que seja indicado de outra forma, você deve estar conectado AWS Management Console na região de origem da sua zona de destino e estar

conectado como usuário do IAM ou usuário no IAM Identity Center com permissões administrativas para a conta de gerenciamento que contém sua zona de destino.

> **Warning**
>
> Essas são ações destrutivas que podem introduzir mudanças na governança em sua configuração do AWS Control Tower. Não podem ser desfeitos.

Tópicos

- Excluir SCPs
- Excluir StackSets e acumular
- Exclua buckets do Amazon S3 na conta do Log Archive
- Remover um portfólio e um produto da Account Factory
- Remova as funções e políticas do AWS Control Tower
- Ajuda de recursos do AWS Control Tower

## Excluir SCPs

O AWS Control Tower usa políticas de controle de serviços (SCPs) para seus controles. Este procedimento explica como excluir os SCPs especificamente relacionados ao AWS Control Tower.

Para excluir AWS Organizations SCPs

1. Abra o console do Organizations em https://console.aws.amazon.com/organizations/.
2. Abra a guia Policies (Políticas), encontre as políticas de controle de serviço (SCPs) que tenham o prefixo aws-guardrails- e faça o seguinte para cada SCP:
   a. Desanexe a SCP da UO associada.
   b. Exclua a SCP.

## Excluir StackSets e acumular

O AWS Control Tower usa StackSets e empilha para implantar controles Regras do AWS Config relacionados à sua landing zone. Os procedimentos a seguir demonstram passo a passo como excluir esses recursos específicos.

Para excluir AWS CloudFormation StackSets

1. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
2. No menu de navegação à esquerda, escolha StackSets.
3. Para cada um StackSet com o prefixo AWSControlTower, faça o seguinte. Se você tiver muitas contas em um StackSet, isso pode levar algum tempo.
    a. Escolha o específico na StackSet tabela no painel. Isso abre a página de propriedades para isso StackSet.
    b. Na parte inferior da página, na tabela Stacks, faça um registro dos IDs de AWS conta de todas as contas na tabela. Copie a lista de todas as contas.
    c. Em Ações, escolha Excluir pilhas de StackSet.
    d. Em Definir opções de implantação, em Locais de implantação, escolha Implantar pilhas em contas.
    e. No campo de texto, insira os IDs da AWS conta dos quais você fez um registro na etapa 3.b, separados por vírgulas. Por exemplo: *123456789012*, *098765431098* e assim por diante.
    f. Em Specify regions (Especificar regiões), escolha Add all (Adicionar tudo), deixe o restante dos parâmetros na página definidos como os padrões e escolha Next (Próximo).
    g. Na página Review (Revisar), examine as opções e escolha Delete stacks (Excluir pilhas).
    h. Na página de StackSet propriedades, você pode começar esse procedimento novamente para sua outra pessoa StackSets.
4. O processo é concluído quando os registros na tabela Pilhas das diferentes páginas de StackSets propriedades estão vazios.
5. Quando os registros na tabela de Pilhas estiverem vazios, escolha Excluir StackSet.

Para excluir AWS CloudFormation pilhas

1. Abra o AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
2. No painel de pilhas, pesquise todas as pilhas com o prefixo. AWSControlTower
3. Para cada pilha na tabela, faça o seguinte:
    a. Marque a caixa de seleção ao lado do nome da pilha.
    b. No menu Actions (Ações), escolha Delete Stack (Excluir pilha).

c. Na caixa de diálogo aberta, examine as informações para ter certeza da precisão e escolha Yes, Delete (Sim, excluir).

### Exclua buckets do Amazon S3 na conta do Log Archive

Os procedimentos a seguir orientam você sobre como fazer login na conta de arquivamento de registros como usuário do IAM Identity Center no AWSControlTowerExecutiongrupo e, em seguida, excluir os buckets do Amazon S3 em sua conta de arquivamento de registros.

Para fazer login na conta de arquivamento de logs com as permissões certas

1. Abra o console do Organizations em https://console.aws.amazon.com/organizations/.
2. Na guia Accounts (Contas), encontre a conta Log archive (Arquivamento de logs).
3. No painel à direita aberto, anote o número da conta de arquivamento de logs.
4. Na barra de navegação, escolha o nome da conta para abrir o menu da conta.
5. Selecione Switch Role (Mudar de função).
6. Na página aberta, forneça o número da conta de arquivamento de logs em Account (Conta).
7. Em Função, insira AWSControlTowerExecution.
8. O Display Name (Nome de exibição) é preenchido com texto.
9. Escolha a Color (Cor) favorita.
10. Selecione Switch Role (Mudar de função).

Para excluir buckets do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Procure nomes de bucket que contenham aws-controltower.
3. Para cada bucket na tabela, faça o seguinte:

   a. Escolha a caixa de seleção do bucket na tabela.

   b. Escolha Excluir.

   c. Na caixa de diálogo aberta, examine as informações para ter certeza de que elas sejam precisas, digite o nome do bucket para confirmar e escolha Confirm (Confirmar).

### Remover um portfólio e um produto da Account Factory

O procedimento a seguir explica como fazer login como usuário do IAM Identity Center no AWSServiceCatalogAdminsgrupo e depois limpar seu portfólio e produtos do Account Factory.

Para entrar na sua conta de gerenciamento com as permissões corretas

1. Acesse o URL do portal do usuário em *directory-id*.awsapps.com/start
2. Em AWS Conta, encontre a conta de gerenciamento.
3. Em AWSServiceCatalogAdminFullAccess, escolha Console de gerenciamento para entrar no AWS Management Console como esta função.

Para limpar o Account Factory

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, escolha Portfolios list (Lista de portfólios).
3. Na tabela Portfólios locais, pesquise um portfólio chamado AWS Control Tower Account Factory Portfolio.
4. Escolha o nome desse portfólio para acessar a página de detalhes.
5. Expanda a seção Restrições da página e escolha o botão de rádio para a restrição com o nome do produto AWS Control Tower Account Factory.
6. Escolha REMOVE CONSTRAINTS (REMOVER RESTRIÇÕES).
7. Na caixa de diálogo exibida, examine as informações para verificar se elas estão precisas e escolha CONTINUE (CONTINUAR).
8. Na seção Produtos da página, escolha o botão de rádio para o produto chamado AWS Control Tower Account Factory.
9. Escolha REMOVE PRODUCT (REMOVER PRODUTO).
10. Na caixa de diálogo exibida, examine as informações para verificar se elas estão precisas e escolha CONTINUE (CONTINUAR).
11. Expanda a seção Users, Groups, and Roles (Usuários, grupos e funções) e escolha as caixas de seleção de todos os registros nessa tabela.
12. Escolha REMOVE USERS, GROUP OR ROLE (REMOVER USUÁRIOS, GRUPOS OU FUNÇÕES).
13. Na caixa de diálogo exibida, examine as informações para verificar se elas estão precisas e escolha CONTINUE (CONTINUAR).

14. No menu de navegação à esquerda, escolha Portfolios list (Lista de portfólios).
15. Na tabela Portfólios locais, pesquise um portfólio chamado AWS Control Tower Account Factory Portfolio.
16. Escolha o botão de opção desse portfólio e escolha DELETE PORTFOLIO (EXCLUIR PORTFÓLIO).
17. Na caixa de diálogo exibida, examine as informações para verificar se elas estão precisas e escolha CONTINUE (CONTINUAR).
18. No menu de navegação à esquerda, escolha Product list (Lista de produtos).
19. Na página de produtos administrativos, pesquise o produto chamado AWS Control Tower Account Factory.
20. Escolha o produto para abrir a página Admin product details (Detalhes do produto de administrador).
21. Em Actions (Ações), escolha Delete product (Excluir produto).
22. Na caixa de diálogo exibida, examine as informações para verificar se elas estão precisas e escolha CONTINUE (CONTINUAR).

### Remova as funções e políticas do AWS Control Tower

Esses procedimentos explicam como limpar as funções e políticas que o AWS Control Tower criou quando sua landing zone foi configurada ou posteriormente.

#### Para excluir a função do IAM Identity Center AWSServiceCatalogEndUserAccess

1. Abra o AWS IAM Identity Center console em https://console.aws.amazon.com/singlesignon/.
2. Mude sua AWS região para sua região de origem, que é a região em que você configurou inicialmente o AWS Control Tower.
3. No menu de navegação à esquerda, escolha AWS contas.
4. Escolha o link da sua conta de gerenciamento.
5. Escolha a lista suspensa para Conjuntos de permissões, selecione e, em seguida AWSServiceCatalogEndUserAccess, escolha Remover.
6. Escolha AWS contas no painel esquerdo.
7. Abra a guia Permission sets (Conjuntos de permissões).
8. Selecione AWSServiceCatalogEndUserAccesse exclua.

Para excluir funções do IAM

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No menu de navegação à esquerda, escolha Roles (Funções).
3. Na tabela, pesquise funções com o nome AWSControlTower.
4. Para cada função na tabela, faça o seguinte:
    a. Escolha a caixa de seleção da função.
    b. Clique em Excluir função.
    c. Na caixa de diálogo aberta, examine as informações para verificar se elas estão precisas e escolha Yes, delete (Sim, excluir).

Para excluir políticas do IAM

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No menu de navegação à esquerda, escolha Policies (Políticas).
3. Na tabela, pesquise políticas com o nome AWSControlTower.
4. Para cada política na tabela, faça o seguinte:
    a. Marque a caixa de seleção da política.
    b. Escolha Policy actions (Ações da política) e Delete (Excluir) no menu suspenso.
    c. Na caixa de diálogo aberta, examine as informações para verificar se elas estão precisas e escolha Delete (Excluir).

Ajuda de recursos do AWS Control Tower

Se você encontrar algum problema que não consiga resolver ao remover os recursos do AWS Control Tower, entre em contato com o AWS Support.

## Como descomissionar uma landing zone

Para descomissionar sua zona de pouso do AWS Control Tower, siga o procedimento fornecido aqui.

> **Note**
>
> Recomendamos que você desgerencie suas contas inscritas antes da desativação.

1. Navegue até a página Landing Zone Settings no console do AWS Control Tower.
2. Escolha Decommission your landing zone (Desativar sua zona de destino) na seção Decommission your landing zone (Desativar sua zona de destino).
3. Uma caixa de diálogo é exibida, explicando a ação que você está prestes a executar, com um processo de confirmação necessário. Para confirmar sua intenção de desativação, você deve selecionar todas as caixas e digitar a confirmação conforme solicitado.

   > **Important**
   >
   > O processo de desativação não pode ser desfeito.

4. Se você confirmar sua intenção de descomissionar sua landing zone, você será redirecionado para a página inicial do AWS Control Tower enquanto o descomissionamento estiver em andamento. O processo pode exigir até duas horas.
5. Quando o descomissionamento for bem-sucedido, você deverá excluir manualmente os recursos restantes antes de configurar uma nova landing zone no console do AWS Control Tower. Esses recursos restantes incluem alguns buckets, organizações e grupos de CloudWatch logs de registros específicos do Amazon S3.

   > **Note**
   >
   > Essas ações podem ter consequências significativas para suas atividades de cobrança e conformidade. Por exemplo, a não exclusão desses recursos pode resultar em cobranças inesperadas.

   Para obter mais informações sobre como excluir recursos manualmente, consulte Sobre a remoção de recursos do AWS Control Tower.
6. Se você pretende configurar um novo landing zone em uma nova AWS região, siga esta etapa adicional. Digite o seguinte comando por meio da CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

Tarefas de limpeza manual necessárias após o descomissionamento

- Você deve especificar endereços de e-mail diferentes para o arquivo de log e as contas de auditoria se criar uma nova landing zone após descomissionar uma, ou seguir o procedimento para trazer seu próprio arquivo de log ou contas de auditoria existentes.
- O grupo de CloudWatch registros de registros`aws-controltower/CloudTrailLogs`,, deve ser excluído manualmente antes de você configurar outra landing zone.
- Os dois buckets do Amazon S3 com nomes reservados para registros devem ser removidos ou renomeados manualmente.
- Você deve excluir ou renomear manualmente as unidades organizacionais de Segurança e Sandbox existentes.

> **Note**
>
> Antes de excluir a organização OU do AWS Control Tower Security, você deve primeiro excluir as contas de registro e auditoria, mas não a conta de gerenciamento. Para excluir essas contas, você deve Quando fazer login como usuário root na conta de auditoria e na conta de registro e excluí-las individualmente.

- Talvez você queira excluir manualmente a configuração AWS IAM Identity Center (do IAM Identity Center) do AWS Control Tower, mas você pode continuar com a configuração atual do IAM Identity Center.
- Talvez você queira remover a VPC criada pela AWS Control Tower e remover o conjunto de CloudFormation pilhas da AWS associado.
- Antes de configurar um novo landing zone em uma nova AWS região, você deve seguir estas etapas adicionais.
  - Digite o seguinte comando por meio da CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - Exclua a regra gerenciada restante, chamada`AWSControlTowerManagedRule`, das contas compartilhadas e membros de todas as regiões governadas. `AWSControlTowerManagedRule`é uma EventBridge regra da Amazon.

# Configuração após o descomissionamento de uma landing zone

Após desativar a zona de destino, não é possível executar a configuração com êxito novamente até que a limpeza manual esteja concluída. Além disso, sem a limpeza manual desses recursos restantes, você pode ter cobranças inesperadas. Você deve atentar-se às seguintes questões:

- A conta de gerenciamento da AWS Control Tower faz parte da AWS Control Tower Root OU. Certifique-se de que essas funções e políticas do IAM sejam removidas da conta de gerenciamento:
  - Funções:
    - `AWSControlTowerAdmin`
    - `AWSControlTowerCloudTrailRole`
    - `AWSControlTowerStackSetRole`
  - Políticas:
    - `AWSControlTowerAdminPolicy`
    - `AWSControlTowerCloudTrailRolePolicy`
    - `AWSControlTowerStackSetRolePolicy`
- Talvez você queira excluir ou atualizar a configuração existente do IAM Identity Center para o AWS Control Tower antes de criar uma landing zone novamente, mas não é necessário excluí-la.
- Talvez você queira remover a VPC criada pelo AWS Control Tower.
- A configuração falhará se os endereços de e-mail especificados para as contas de registro ou auditoria estiverem associados a uma AWS conta existente. Você pode fechar as AWS contas ou usar endereços de e-mail diferentes para configurar uma landing zone novamente. Como alternativa, você pode reutilizar essas contas compartilhadas existentes, com o recurso que permite que você traga suas próprias contas de registro e auditoria. Para ter mais informações, consulte Considerações sobre como trazer contas de segurança ou registro existentes.
- A configuração falhará se os buckets do Amazon S3 com os seguintes nomes reservados já existirem na conta de registro:
  - `aws-controltower-logs-{accountId}-{region}` (usado para o bucket de registro).
  - `aws-controltower-s3-access-logs-{accountId}-{region}` (usado para o bucket de acesso de registro).

Você deve renomear ou remover esses buckets, ou usar uma conta diferente para o registro.

- A configuração falhará se a conta de gerenciamento tiver o grupo de registros existente,`aws-controltower/CloudTrailLogs`, em CloudWatch Registros. Você deve renomear ou remover o grupo de logs.

### Antes de configurar um novo Região da AWS

Se você pretende configurar um novo landing zone em uma nova AWS região, siga estas etapas adicionais.

- Digite o seguinte comando por meio da CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Exclua a regra gerenciada restante, chamada`AWSControlTowerManagedRule`, das contas compartilhadas e membros de todas as regiões governadas.

> **Note**
>
> Você não pode configurar uma nova landing zone em uma organização com OUs de alto nível denominadas Security ou Sandbox. É necessário renomear ou remover essas UOs para configurar uma zona de destino novamente.

# Solução de problemas

Se você encontrar problemas ao usar o AWS Control Tower, poderá usar as informações a seguir para resolvê-los de acordo com nossas melhores práticas. Se os problemas que você encontrar estiverem fora do escopo das informações a seguir ou se persistirem após você tentar resolvê-los, entre em contato com o AWS Support.

## Falha na inicialização da zona de destino

Causas comuns de falha na execução da zona de destino:

- Falta de resposta a uma mensagem de e-mail de confirmação.
- AWS CloudFormation StackSet falha.

Mensagens de e-mail de confirmação: se sua conta de gerenciamento tiver menos de uma hora, você poderá encontrar problemas ao criar contas adicionais.

Medida a ser tomada

Se você encontrar esse problema, verifique seu e-mail. Você pode ter recebido um e-mail de confirmação que está aguardando resposta. Como alternativa, recomendamos aguardar uma hora e, depois, tentar novamente. Se o problema persistir, entre em contato com o AWS Support.

Falha StackSets: outra possível causa da falha no lançamento do landing zone é a AWS CloudFormation StackSet falha. AWS As regiões do Security Token Service (STS) devem estar habilitadas na conta de gerenciamento de todas as AWS regiões que o AWS Control Tower está governando, para que o provisionamento possa ser bem-sucedido; caso contrário, os conjuntos de pilhas não serão iniciados.

Medida a ser tomada

Certifique-se de habilitar todas as regiões de endpoint do AWS Security Token Service (STS) necessárias antes de iniciar o AWS Control Tower.

Para ver uma lista do Regiões da AWS que o AWS Control Tower suporta, consulteComo AWS as regiões funcionam com a AWS Control Tower.

# Erro na zona de pouso não atualizada

Se você não atualizou sua landing zone recentemente, você pode receber uma mensagem de erro ao tentar recuperar o acesso ao AWS Control Tower. Você pode ver uma mensagem de erro semelhante a esta:

```
Unable to access Control Tower
```

Sua conta ficou inativa por muito tempo. Devido à inatividade, você deve atualizar sua landing zone para acessar o AWS Control Tower.

No entanto, a atualização da sua landing zone pode falhar.

Etapas a serem tomadas

Entre na conta de gerenciamento da sua organização e entre como usuário root. Seu usuário do IAM ou usuário no IAM Identity Center deve ter permissões de administrador do AWS Control Tower e fazer parte do AWSControlTowerAdminsgrupo. Em seguida, tente atualizar novamente.

# Falha no provisionamento de novas contas

Se você encontrar esse problema, verifique essas causas comuns.

Ao preencher o formulário de provisionamento de conta, você pode ter:

- especificado tagOptions,
- habilitado notificações do SNS,
- habilitado notificações de produtos provisionados.

Tente provisionar sua conta novamente, sem especificar nenhuma dessas opções. Para ter mais informações, consulte Provisionar contas com AWS Service Catalog Account Factory .

Outras causas comuns de falha:

- Se você criou um plano de produto provisionado (para exibir alterações de recursos), seu provisionamento de conta pode permanecer em um estado In progress (Em andamento) indefinidamente.
- A criação de uma nova conta no Account Factory falhará enquanto outras alterações de configuração do AWS Control Tower estiverem em andamento. Por exemplo, enquanto um

processo estiver em execução para adicionar um controle a uma OU, o Account Factory exibirá uma mensagem de erro se você tentar provisionar uma conta.

Para verificar o status de uma ação anterior no AWS Control Tower

- Navegue até AWS CloudFormation > StackSets
- Verifique cada conjunto de pilhas relacionado ao AWS Control Tower (prefixo: ""“AWSControlTower)
- Procure AWS CloudFormation StackSets as operações que ainda estão em execução.

Se o provisionamento de sua conta demorar mais de uma hora, é melhor encerrar o processo de provisionamento e tentar novamente.

## Falha ao registrar uma conta existente

Se você tentar registrar uma AWS conta existente uma vez e essa inscrição falhar, ao tentar pela segunda vez, a mensagem de erro poderá indicar que o conjunto de pilhas existe. Para continuar, é necessário remover o produto provisionado na Fábrica de contas.

Se o motivo da primeira falha de registro foi que você esqueceu de criar a função `AWSControlTowerExecution` na conta com antecedência, a mensagem de erro que você receberá corretamente informará que a função deve ser criada. No entanto, ao tentar criar a função, é provável que você receba outra mensagem de erro informando que o AWS Control Tower não pôde criar a função. Esse erro ocorre porque o processo foi parcialmente concluído.

Nesse caso, é necessário executar duas etapas de recuperação antes de continuar a registrar sua conta existente. Primeiro, você deve encerrar o produto provisionado pelo Account Factory por meio do console. AWS Service Catalog Em seguida, você deve usar o AWS Organizations console para mover manualmente a conta da OU e voltar para a raiz. Depois disso, crie a função `AWSControlTowerExecution` na conta e preencha o formulário Enroll account (Registrar conta) novamente.

Outra possível causa da falha na inscrição é que a conta tem recursos do AWS Config existentes. Nesse caso, consulte Inscrever contas que tenham AWS Config recursos existentes para obter instruções sobre como você pode modificar seus recursos existentes.

# Não é possível atualizar uma conta da Fábrica de contas

Quando uma conta está em um estado inconsistente, ela não pode ser atualizada com sucesso no Account Factory ou AWS Service Catalog.

Caso 1: Você pode encontrar uma mensagem de erro semelhante a esta:

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

Causa comum: o AWS Control Tower sempre remove a VPC AWS padrão durante o provisionamento inicial. Para ter uma VPC AWS padrão em uma conta, você deve adicioná-la após a criação da conta. A AWS Control Tower tem sua própria VPC padrão que substitui a AWS VPC padrão, a menos que você configure o Account Factory da maneira que o passo a passo mostra, para que a AWS Control Tower não provisione nenhuma VPC. A conta não tem uma VPC. Você precisaria adicionar novamente a VPC AWS padrão se quiser usá-la.

No entanto, o AWS Control Tower não é compatível com a VPC AWS padrão. A implantação de uma VPC faz com que a conta entre em um estado `Tainted`. Quando está nesse estado, você não pode atualizar a conta por meio de AWS Service Catalog.

Ação a ser executada: você deve excluir a VPC padrão adicionada e, depois, conseguirá atualizar a conta.

> **Note**
>
> O `Tainted` estado causa um problema subsequente: uma conta que não está atualizada pode impedir a ativação de controles na OU da qual ela faz parte.

Caso 2: Você pode ver uma mensagem de erro semelhante a esta:

```
AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.
```

Causa comum: você tentou mover uma conta de uma OU registrada para outra, mas as regras antigas AWS do Config permanecem. A conta está em um estado inconsistente.

Ação a ser tomada:

Se a mudança de conta foi planejada:

- Encerre a conta no Service Catalog.
- Inscreva-o novamente.
- Contexto/impacto: as regras de AWS Config implantadas não correspondem à configuração ditada pela OU de destino.
- AWS As regras de Config podem permanecer da OU anterior, causando gastos não intencionais.
- As tentativas de reinscrever ou atualizar a conta falharão devido a conflitos de nomenclatura de recursos.

Se a mudança da conta não foi intencional:

- Retorne a conta para sua OU original.
- Atualize a conta no Service Catalog.
- Nos parâmetros de inicialização, insira a OU na qual a conta estava originalmente.
- Contexto/impacto: se a conta não for devolvida à sua OU original, seu estado será inconsistente com os controles ditados pela nova OU em que ela se encontra.
- Atualizar uma conta não é uma remediação válida, pois não exclui as AWS Config regras associadas à OU anterior.

## Não é possível atualizar a zona de aterrissagem

O AWS Control Tower não reverte para uma versão anterior da landing zone se uma atualização falhar. Você pode encontrar seu landing zone em um estado indeterminado. Em caso afirmativo, entre em contato com AWS o suporte.

As atualizações da zona de pouso podem falhar por vários motivos.

- Pré-requisitos não atendidos
- AWS Config existem recursos em determinadas contas
- Existem contas fechadas

Pré-requisitos não atendidos

A atualização da zona de pouso deve atender aos mesmos pré-requisitos da configuração da zona de pouso. Antes de atualizar, revise as verificações de pré-lançamento.

AWS Config existem recursos nas contas da OU de segurança

Não adicione AWS Config recursos em suas contas de arquivamento de auditoria e registro. O processo de atualização da landing zone não pode ser concluído com esses recursos presentes. Essas restrições são semelhantes às de cadastrar uma conta ou configurar uma landing zone pela primeira vez. Para obter mais informações, consulte Inscrever contas que tenham AWS Config recursos existentes.

Existem contas fechadas

Quando uma conta está no estado Fechado ou Suspenso, você pode encontrar um problema ao tentar atualizar sua landing zone. Você deve excluir o produto provisionado em cada conta fechada antes de realizar uma atualização na landing zone.

Na página do produto AWS Service Catalog provisionado, você pode ver uma mensagem de erro semelhante a esta:

```
AWSControlTowerExecution role can't be assumed on the account.
```

Causa comum: você suspendeu uma conta sem excluir o produto provisionado.

Ação a ser tomada: se você ver esse erro, você tem duas opções:

1. Entre em contato com o AWS Support e reabra a conta, exclua o produto provisionado e feche a conta novamente.
2. Remova os recursos do StackSets que ficaram órfãos devido ao encerramento da conta. (Essa opção está disponível somente se houver instâncias no estado atual que você não está removendo.) StackSets

Para remover os recursos do StackSets, faça o seguinte para cada conta fechada:

- Acesse cada uma das AWS Control Tower StackSets e remova-as StackInstances de todas as regiões da conta que foi fechada.
- IMPORTANTE: Escolha a opção Retain Stack para StackSet remover somente as instâncias da pilha. StackSet não pode assumir uma função da conta fechada, então ela falhará se tentar assumir a `AWSControlTowerExecution` função, o que levará à mensagem de erro que você recebeu.

# Erro de falha que menciona AWS Config

Se AWS Config estiver habilitado em qualquer AWS região suportada pelo AWS Control Tower, você poderá receber uma mensagem de erro porque uma pré-verificação falhou. A mensagem pode parecer não explicar o problema adequadamente, devido a algum comportamento subjacente do AWS Config.

É possível receber uma mensagem de erro semelhante a uma destas:

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

Causa comum: quando o AWS Config serviço é ativado em uma AWS conta, ele cria um gravador de configuração e um canal de entrega com um nome padrão. Se você desativar o AWS Config serviço por meio do console, ele não excluirá o gravador de configuração nem o canal de entrega. Você deve excluí-los por meio da CLI ou modificá-los para uso do AWS Control Tower. Se o AWS Config serviço estiver habilitado em qualquer uma das regiões suportadas pelo AWS Control Tower, isso pode resultar nessa falha.

Se a conta tiver recursos do AWS Config existentes, consulte Inscrever contas que tenham AWS Config recursos existentes para obter instruções sobre como você pode modificar seus recursos existentes.

Ação a ser tomada: exclua o gravador de configuração e o canal de entrega em todas as regiões com suporte. Desabilitar o AWS Config não é suficiente, o gravador de configuração e o canal de entrega devem ser excluídos por meio da CLI. Depois de excluir o gravador de configuração e o canal de entrega da CLI, você pode tentar novamente iniciar o AWS Control Tower e registrar a conta.

Se você estiver no processo de implantação de um produto provisionado, deverá excluí-lo antes de tentar novamente. Caso contrário, você poderá ver uma mensagem de erro semelhante a esta:

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

Na mensagem, *Stackname*especifica o nome da pilha.

Aqui estão alguns exemplos de comandos da AWS Config CLI que você pode usar para determinar o status do gravador de configuração e do canal de entrega.

Comandos de exibição:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

Comandos de exclusão:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Para obter mais informações, consulte a AWS Config documentação

- Gerenciando o gravador de configuração (AWS CLI)
- Gerenciando o canal de entrega

## Nenhum erro de caminhos de inicialização encontrado

Ao tentar criar uma nova conta, é possível ver uma mensagem de erro semelhante a esta:

```
No launch paths found for resource: prod-dpqqfywxxxx
```

Essa mensagem de erro é gerada pelo AWS Service Catalog, que é o serviço integrado que ajuda a provisionar contas no AWS Control Tower.

Causas comuns:

- Você pode estar logado como root. O AWS Control Tower não suporta a criação de contas quando você está logado como usuário root.
- Seu usuário do IAM Identity Center não foi adicionado ao grupo de permissões apropriado. Talvez seja necessário adicionar seu usuário do IAM Identity Center a um desses grupos de permissão: AWSAccountFactory(para acesso do usuário final) ou AWSServiceCatalogAdmins(para acesso de administrador).
- Se você estiver autenticado como usuário do IAM, deverá adicioná-lo ao AWS Service Catalog portfólio para que ele tenha as permissões corretas.
- Esse problema também ocorre se você tiver as permissões corretas, mas o desvio do AWS Control Tower for detectado e um reparo do desvio for necessário. Para reparar a maioria dos tipos de deriva, escolha Redefinir na página de configurações da zona de pouso.

## Recebeu um erro de permissões insuficientes

É possível que sua conta não tenha as permissões necessárias para realizar determinados trabalhos em determinados casos AWS Organizations. Se você encontrar o seguinte tipo de erro, verifique todas as áreas de permissões, como as permissões do IAM ou do IAM Identity Center, para garantir que sua permissão não esteja sendo negada nesses locais:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Se você acredita que seu trabalho exige a ação que você está tentando e não consegue localizar nenhuma restrição relevante, entre em contato com o administrador do sistema ou com o Support AWS .

## Os controles de detetive não estão entrando em vigor nas contas

Se você expandiu recentemente sua implantação do AWS Control Tower para uma nova AWS região, os controles de detetive recém-aplicados não entrarão em vigor nas novas contas que você criar em qualquer região até que as contas individuais dentro das OUs governadas pela AWS Control Tower sejam atualizadas. Os controles de detetive existentes sobre contas existentes ainda estão em vigor.

Se você tentar ativar um controle de detetive antes de atualizar suas contas, poderá ver uma mensagem de erro semelhante a esta:

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

Ação a realizar: atualizar contas.

Para atualizar suas contas a partir do console do AWS Control Tower, consulteQuando atualizar a AWS Control Tower OUs e as contas.

Para atualizar várias contas individuais de forma programática, você pode usar as APIs e AWS Service Catalog a AWS CLI para automatizar as atualizações. Para obter mais informações sobre como abordar o processo de atualização, consulte Passo a passo em vídeo.  Você pode substituir a UpdateProvisionedProductAPI pela ProvisionProductAPI mostrada no vídeo.

Se você tiver mais dificuldades em ativar os controles de detetive em suas contas, entre em contato com o AWS Support.

## Erro de taxa excedida retornado pela API AWS Organizations

Possível causa

Sua carga de trabalho estava em execução enquanto o AWS Control Tower executava uma verificação diária para verificar se seus SCPs se desviaram.

Etapas a seguir

Se você encontrar uma limitação ou `rate exceeded` erro de API, tente estas etapas:

- Execute suas cargas de trabalho em um horário diferente. (Consulte o cronograma de verificação de invariância de SCP do AWS Control Tower por região para descobrir quando a AWS Control Tower executa suas verificações de auditoria.)
- Se você estiver chamando as APIs diretamente por meio de HTTP: use o AWS SDK, que repete automaticamente as ações com falha
- Solicite um aumento de limite por meio de Service Quotas and Support AWS

Um exemplo de instruções de solução de problemas para limitação de API no Elastic Beanstalk pode ser encontrado aqui: `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

# Falha ao mover uma conta do Account Factory diretamente de uma zona de pouso da AWS Control Tower para outra zona de pouso da AWS Control Tower

> **Warning**
>
> Essa prática não atende ao pré-requisito para o registro de contas elegíveis, porque as contas elegíveis devem fazer parte da mesma organização geral da AWS, e cada organização pode ter apenas uma landing zone. Se você tentou fazer essa ação e está recebendo várias mensagens de erro, aqui estão algumas informações que podem ser úteis.

Para mover uma conta que você provisionou por meio do Account Factory para outra landing zone gerenciada pelo AWS Control Tower, em outra conta de gerenciamento, você deve remover todas as funções do IAM e as pilhas associadas a essa conta da OU original. Remova esses recursos de todas as regiões nas quais a conta está implantada.

> **Note**
>
> A melhor maneira de remover os recursos é desprovisionar a conta em sua OU original antes de tentar movê-la.

Se você não remover os recursos, a inscrição na nova OU falhará, de forma espetacular. Você pode encontrar uma ou mais mensagens de erro e continuará recebendo mensagens de erro semelhantes até que as funções e pilhas restantes sejam removidas de cada região em que a conta foi implantada.

Sempre que receber uma mensagem de erro, você deve remover a conta da nova OU, excluir o recurso antigo que é o assunto da mensagem de erro e, em seguida, tentar mover a conta de volta para a nova OU. Esse processo removing-and-deleting deve ser repetido para cada recurso restante, para cada região em que a conta foi implantada, possivelmente 10 ou 20 vezes. Esses

erros repetidos ocorrem porque a conta foi provisionada em uma OU com um SCP que impede a exclusão da função do IAM. Você pode encurtar o processo de recuperação excluindo todos os recursos da conta antes de tentar novamente.

Os exemplos abaixo representam os tipos de mensagens de falha que você pode receber se as funções e pilhas não excluídas permanecerem. Você provavelmente verá uma dessas mensagens por vez, a cada vez que tentar registrar a conta, desde que os recursos antigos permaneçam.

Os valores das cadeias de caracteres de ID do recurso foram modificados para os exemplos. Seus valores não serão os mesmos em uma mensagem de erro que você possa receber. Você pode ver uma mensagem semelhante aos seguintes exemplos:

- `AWS Control Tower cannot create the IAM role aws-controltower-AdministratorExecutionRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ConfigRecorderRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ForwardSnsNotificationRole because the role already exists. To continue, delete the existing IAM role and try again.`

Ou você pode ver uma mensagem de erro sobre uma falha no conjunto de pilhas, semelhante a esta:

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
```

```
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

Depois que todos os recursos restantes forem removidos da primeira OU, você poderá convidar, provisionar ou inscrever a conta na nova OU com sucesso.

## AWS Support

Se pretender mover as suas contas-membro existentes para um plano de suporte diferente, você poderá iniciar sessão em cada conta com credenciais de conta raiz, comparar planos, e definir o nível de suporte que preferir.

Recomendamos atualizar a MFA e os contatos de segurança da conta quando fizer alterações no plano de suporte.

# Tipos de linhas de base

Uma linha de base no AWS Control Tower é um grupo de recursos e configurações específicas que você pode aplicar a um alvo. A meta básica mais comum pode ser uma unidade organizacional (OU). Por exemplo, você pode habilitar uma linha de base com uma OU selecionada como destino para registrar essa OU no AWS Control Tower.

Durante a configuração da zona de pouso, a meta básica pode ser uma conta compartilhada ou a zona de pouso como um todo. Certas linhas de base podem ser habilitadas e atualizadas com base nas configurações e configurações do seu landing zone. O AWS Control Tower cria e implanta os recursos no destino da forma que a linha de base especifica.

Quando você ativa uma linha de base para um alvo, a linha de base é representada como um AWS CloudFormation recurso, chamado de recurso. `EnabledBaseline`

O AWS Control Tower inclui quatro tipos essenciais de linhas de base:

- Um tipo pode ser aplicado a uma OU registrada no AWS Control Tower ou a uma OU que você pretende registrar aplicando a linha de base.
- Três tipos de linha de base podem ser aplicados a uma zona de pouso ou conta compartilhada, durante a configuração inicial ou durante uma atualização da zona de pouso.

Tipo de linha de base que se aplica no nível da OU, para registrar e atualizar OUs

- Nome: `AWSControlTowerBaseline`

  Descrição: configura recursos e controles obrigatórios para contas de membros dentro da OU de destino, necessários para a governança do AWS Control Tower.

  Consideração: Essa linha de base mantém as configurações da zona de pouso Region Deny Control. Em outras palavras, se uma região não é permitida no nível da landing zone, essa região não é permitida para aquela OU quando você chama a `EnableBaseline` API para registrar uma OU.

  > **Note**
  >
  > A região de nível da UA nega o controle não tem como permitir regiões que a região de landing zone nega o controle não permite.

Para obter mais informações, consulte Como os SCPs funcionam com a negação na AWS Organizations documentação.

Recomendação: recomendamos que você confirme as regiões nas quais sua OU de destino pode estar executando cargas de trabalho e verifique os resultados em relação à região de negação de controle da região da landing zone, antes de chamar a `EnableBaseline` API da OU, caso contrário, você poderá perder o acesso aos recursos em determinadas regiões.

> **Note**
>
> As linhas de base da zona de aterrissagem se comportam de maneira diferente das linhas de base do nível da OU.

O AWS Control Tower habilita as linhas de base que se aplicam automaticamente no nível da zona de pouso, como parte do processo de configuração e atualização da zona de pouso. As linhas de base da sua zona de pouso podem mudar conforme você altera as configurações da sua zona de pouso. Por exemplo, se você optar pelo IAM Identity Center, o AWS Control Tower poderá habilitar a versão mais recente da `IdentityCenterBaseline` linha de base em sua landing zone.

Você pode ver as linhas de base habilitadas para sua landing zone com a chamada de `ListEnabledBaselines` API.

Tipos de linha de base que podem se aplicar à sua landing zone ou contas compartilhadas

- Nome: `AuditBaseline`

  Descrição: configura recursos para monitorar a segurança e a conformidade das contas em sua organização. Você não pode alterar essa linha de base, ela é implantada pelo AWS Control Tower.
- Nome: `LogArchiveBaseline`

  Descrição: configura um repositório central para registros de atividades de API e configurações de recursos de contas em sua organização. Você não pode alterar essa linha de base, ela é implantada pelo AWS Control Tower.
- Nome: `IdentityCenterBaseline`

Descrição: configura recursos compartilhados para o IAM Identity Center, que prepara o `AWSControlTowerBaseline` para configurar o acesso ao Identity Center para contas.

Consideração: essa linha de base funciona somente quando você seleciona o IAM Identity Center como seu provedor de identidade no momento em que configurou sua zona de pouso inicialmente, ou se você posteriormente altera as configurações da zona de destino para habilitar o IAM Identity Center para sua zona de pouso. Se você estiver usando um provedor de identidade diferente, não terá acesso para ativar essa linha de base.

## Inscrição parcial de contas

Quando você trabalha com linhas de base, uma conta pode ser colocada em um estado chamado Parcialmente inscrito.

Esse estado pode ocorrer se você registrar novamente uma OU chamando a `ResetEnabledBaseline` API, porque o AWS Control Tower aplica somente os recursos obrigatórios às contas na OU de destino. Uma conta que não tem os recursos opcionais (controles) de sua OU principal é marcada como Parcialmente inscrita.

Se você mover uma conta não cadastrada para uma OU registrada e, em seguida, chamar a `ResetEnabledBaseline` API na OU para inscrever essa conta, o AWS Control Tower aplicará os recursos associados à à conta recém-inscrita. `AWSControlTowerBaseline` No entanto, os controles opcionais habilitados para essa OU não são aplicados à conta. A conta permanece em um estado parcialmente inscrito.

Para registrar totalmente a conta, escolha Registrar novamente ou Atualizar conta no console. Quando você seleciona essas operações no console, o AWS Control Tower aplica todos os recursos dessa OU à conta recém-cadastrada, incluindo os controles opcionais que são ativados para essa OU.

## Variação nas operações entre o console do AWS Control Tower e as APIs para linhas de base

Quando você altera o status de governança de uma OU, o console do AWS Control Tower executa automaticamente mais operações para você, em comparação com a mudança da governança por meio das APIs para linhas de base.

Diferenças

- Registro e provisionamento de produtos

  Quando você registra uma OU por meio do console, o AWS Control Tower cria produtos do Service Catalog para as contas dos membros da OU, como parte da inscrição de cada conta. Quando você registra uma OU por meio da `EnableBaseline` API e da`AWSControlTowerBaseline`, o AWS Control Tower não cria produtos provisionados para as contas dos membros na OU.

- Cancele o registro de uma OU

  Sempre que você cancelar o registro de uma OU, primeiro remova todas as contas de membros e OUs aninhadas. Em seguida, o AWS Control Tower remove todos os controles que são aplicados à OU.

  - Se você selecionar Excluir OU da OU do console, o AWS Control Tower cancelará o registro e, em seguida, excluirá a OU da sua organização.
  - No entanto, se você cancelar o registro da OU chamando a `DisableBaseline` API para removê-la `AWSControlTowerBaseline` da OU, o AWS Control Tower não excluirá a OU da sua organização, a OU ainda estará presente na organização, sem registro.

# Linhas de base e padrões de versão

Se sua zona de pouso da AWS Control Tower já estiver configurada e você optar por habilitar uma linha de base da zona de pouso, a AWS Control Tower habilita a versão mais recente da linha de base compatível com a versão da sua zona de pouso. Se você optar por habilitar uma linha de base para uma OU que ainda não esteja registrada na AWS Control Tower, a AWS Control Tower fornecerá automaticamente a versão mais recente compatível da linha de base para essa OU.

# Compatibilidade das linhas de base da OU e das versões do landing zone

As linhas de base do AWS Control Tower permitem que você defina um padrão de governança no nível da OU, em vez de no nível da landing zone, se sua empresa precisar. A linha de base chamada `AWSControlTowerBaseline` está disponível para ajudar a registrar suas OUs no AWS Control Tower.

> **Note**
>
> Uma linha de base é um grupo de controles e recursos que trabalham juntos para estabelecer um ambiente de governança estável em sua landing zone.

Ao habilitar uma linha de base em uma OU, chamando a `EnableBaseline` API na AWS Control Tower, você deve especificar uma versão básica que seja compatível com sua versão atual da zona de pouso do AWS Control Tower. Depois de especificar uma linha de base, todas as contas de membros em uma OU seguem a linha de base fornecida para a OU. Em outras palavras, novas contas são provisionadas com a linha de base atualizada e as contas de membros existentes são governadas de acordo com a nova linha de base.

Se você não selecionar uma linha de base para suas OUs e contas existentes, a versão landing zone determinará toda a postura de governança, por padrão. No entanto, cada OU registrada em sua zona de pouso recebe uma versão de linha de base, que é a linha de base mais recente compatível com a versão atual da sua zona de pouso. Portanto, cada OU e conta de membro inscrito tem uma linha de base associada, mesmo que você nunca atribua uma linha de base especificamente.

Para a linha de base em nível de UO`AWSControlTowerBaseline`, a tabela a seguir mostra a compatibilidade das linhas de base com as versões da zona de pouso do AWS Control Tower.

| Versão de linha de base | Versões da zona de pouso | Plantas incluídas | Controles incluídos | Alteração em relação à linha de base anterior | |
|---|---|---|---|---|---|
| 1,0 | 2,0 a 2,7 | BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELI | Todos os controles obrigatórios | Nenhum | |

| Versão de linha de base | Versões da zona de pouso | Plantas incluídas | Controles incluídos | Alteração em relação à linha de base anterior | |
|---|---|---|---|---|---|
| | | NE_SERVIC E_ROLES, recursos do IAM | | | |
| 2,0 | 2,8 a 2,9 | BP_BASELI NE_CLOUDT RAIL, BP_BASELI NE_CLOUDW ATCH, BP_BASELI NE_CONFIG , BP_BASELI NE_ROLES, BP_BASELI NE_SERVIC E_ROLES, Config SLR, recursos do IAM | Todos os controles obrigatórios | Função AWS Config vinculada ao serviço (SLR) adicionad a e novo esquema Config para usar a SLR | |

| Versão de linha de base | Versões da zona de pouso | Plantas incluídas | Controles incluídos | Alteração em relação à linha de base anterior | |
|---|---|---|---|---|---|
| 3.0 | 3,0 a 3,1 | BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, recursos do IAM | Todos os controles obrigatórios | Novo AWS Config projeto. Altere para registrar recursos globais somente na região de origem. CloudTrail Projeto removido | |
| 4,0 | 3.2 a 3.3 | BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, recursos do IAM | Todos os controles obrigatórios | Novo modelo de SLR | |

Para obter mais informações sobre recursos específicos criados em contas quando você configura sua landing zone, consulte Recursos criados nas contas compartilhadas.

Se você atualizar sua zona de pouso para uma versão que suporte uma versão de **`AWSControlTowerBaseline`** linha de base mais recente, e a nova versão da zona de pouso for compatível com sua versão de linha de base existente, seu estado de OU mudará para Atualização disponível.

- Você pode continuar usando a fábrica de contas e outros recursos sem atualizar a linha de base da OU imediatamente, exceto no caso de uma atualização da landing zone de 2.x para 3.x.
- As novas contas inscritas nesta OU recebem recursos com base na versão básica existente até que a versão base seja atualizada (com o recurso de governança estendida no console ou por meio da `UpdateEnabledBaseline` API).
- Depois de atualizar a versão de linha de base, todas as contas dentro dessa OU recebem recursos com base na nova versão de linha de base.

> **Note**
>
> Se você atualizar sua zona de pouso do AWS Control Tower de qualquer versão 2.X para qualquer versão 3.X, você também deverá atualizar a versão básica em suas OUs, devido à mudança de trilhas em nível de conta para trilhas em nível de organização. AWS CloudTrail No console, sua OU mostrará o status de Atualização necessária.

Considerações sobre as linhas de base

- Se sua OU exigir uma atualização de linha de base, você não poderá provisionar novas contas nem inscrever contas existentes nessa OU.
- Depois de uma atualização da landing zone, se você também planeja atualizar uma linha de base de OU, você deve registrar novamente a OU atualizar sua versão de linha de base de OU programaticamente.
- Recomendamos que você atualize para a linha de base mais compatível com a versão da zona de pouso que está usando, para que você obtenha todos os benefícios da zona de pouso e da linha de base combinadas. Por exemplo, se você atualizar para a versão 3.3 da zona de pouso, poderá continuar usando a linha de base 3.0, mas não obterá todos os benefícios da versão 3.3 da zona de pouso, a menos que também atualize para a linha de base 4.0.

- As atualizações de linha de base não podem ser revertidas.
- A capacitação básica visa uma OU por vez. Portanto, OUs aninhadas não são atualizadas automaticamente quando a OU principal é atualizada. Recomendamos que você atualize a OU principal antes de atualizar as OUs aninhadas.
- Quando você chama a `UpdateEnabledBaseline` API ou registra novamente uma OU a partir do console, a OU retém todos os controles que foram ativados antes da atualização da linha de base.
- Quando várias versões de linha de base são compatíveis com sua versão de landing zone, você deve usar a versão de linha de base mais recente se habilitar uma linha de base em uma OU não gerenciada,.

# Exemplos: registre uma OU do AWS Control Tower somente com APIs

Este guia de exemplos é um documento complementar. Para obter explicações, advertências e mais informações, consulte. Tipos de linhas de base

Pré-requisitos

Você deve ter uma OU existente que não esteja registrada no AWS Control Tower e que você gostaria de registrar. Ou você deve ter uma OU registrada que gostaria de registrar novamente para fins de atualização.

Registre uma OU

1. Verifique se `IdentityCenterBaseline` está habilitado para a landing zone. Em caso afirmativo, obtenha o identificador de linha de base habilitado para o Identity Center.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. Obtenha o ARN da UO de destino.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Obtenha o ARN da linha de base. `AWSControlTowerBaseline`

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Crie a linha de `AWSControlTowerBaseline` base na UO de destino.

   Se a linha de base do Identity Center estiver ativada:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   Se a linha de base do Identity Center não estiver ativada, omita o *`parameters`* sinalizador, da seguinte forma:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Registre novamente uma OU

Depois de fazer atualizações nas configurações da zona de pouso ou atualizar sua versão da zona de pouso, você deve registrar novamente as OUs para fornecer as alterações mais recentes. Siga estas etapas para registrar novamente uma OU programaticamente, redefinindo o recurso associado. `EnabledBaseline`

1. Obtenha o ARN da OU de destino para se registrar novamente.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Obtenha o ARN do `EnabledBaseline` recurso para a UO de destino.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. Redefina a linha de base ativada.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

# Exemplos de uso básico API

Esta seção contém exemplos de parâmetros de entrada e saída para a linha de base APIs do AWS Control Tower.

## `DisableBaseline`

Para obter mais informações sobre essa API operação, consulte DisableBaseline.

`DisableBaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline`saída:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`DisableBaseline`CLIexemplo:

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

## `EnableBaseline`

Para obter mais informações sobre essa API operação, consulte EnableBaseline.

`EnableBaseline`entrada:

```
{
```

```
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`EnableBaseline`saída, retornando um novo recurso:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

`EnableBaseline`CLIexemplo:

Este exemplo mostra a ativação de uma linha de base para um AWS Organizations organização que tem a landing zone ativada para AWS IAMAcesso ao Identity Center, gerenciado pela AWS Control Tower. Para recuperar seu `EnabledBaseline` identificador do Identity Center, você pode chamar o `ListEnabledBaselines`API, filtrando na linha de base do Identity Center: `(arn:aws:controltower:`*`Region`*`::baseline/LN25R72TTG6IGPTQ)`

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

A resposta mostrará o `EnabledBaseline` detalhe, que mostra seu identificador.

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
```

```
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> Anote o ARN valor da resposta e passe esse valor como um parâmetro para ativar a linha de base padrão.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Para uma organização com a landing zone excluída do gerenciamento da AWS Control Tower do IAM Identity Center, ative a linha de base sem o parâmetro.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

## `GetBaseline`

Para obter mais informações sobre essa API operação, consulte GetBaseline.

`GetBaseline`entrada:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline`saída:

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

`GetBaseline`CLIexemplo:

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

## `GetBaselineOperation`

Para obter mais informações sobre essa API operação, consulte GetBaselineOperation.

`GetBaselineOperation`entrada:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`GetBaselineOperation`saída:

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
```

```
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

GetBaselineOperationCLIexemplo:

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

## GetEnabledBaseline

Para obter mais informações sobre essa API operação, consulte GetEnabledBaseline.

GetEnabledBaselineentrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

GetEnabledBaselinesaída:

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
```

```
            }
        ]
    }
}
```

`GetEnabledBaseline`CLIexemplo:

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

## `ListBaselines`

Para obter mais informações sobre essa API operação, consulte ListBaselines.

`ListBaselines`entrada (usando entradas opcionais):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines`saída:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
```

```
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        }
    ]
}
```

`ListBaselines`CLIexemplo:

```
aws controltower list-baselines \
    --region us-west-2
```

## `ListEnabledBaselines`

Para obter mais informações sobre essa API operação, consulte ListEnabledBaselines.

`ListEnabledBaselines`entrada (sem filtros):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`entrada (somente `baselineIdentifiers` filtro):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`entrada (somente `targetIdentifiers` filtro):

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

`ListEnabledBaselines`entrada (`baselineIdentifiers`e `targetIdentifiers` filtros):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`saída:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
```

```
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

CLIexemplo com um tipo de filtro (`baselineIdentifiers`filtro):

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

CLIexemplo usando vários filtros (`baselineIdentifier`e `targetIdentifiers` filtros):

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

## `ResetEnabledBaseline`

Para obter mais informações sobre essa API operação, consulte ResetEnabledBaseline.

`ResetEnabledbaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaseline`saída:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`ResetEnabledBaseline`CLIexemplo:

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

## `UpdateEnabledBaseline`

Para obter mais informações sobre essa API operação, consulte UpdateEnabledBaseline.

`UpdateEnabledBaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`UpdateEnabledBaseline`saída:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`UpdateEnabledBaseline`CLIexemplo:

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
```

```
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

# Informações e links adicionais

Esse tópico inclui links para publicações de blog relevantes, documentação técnica e informações relacionadas que podem ajudá-lo a trabalhar com a AWS Control Tower. As fontes abordam alguns casos de uso comuns e as melhores práticas dos recursos da AWS Control Tower, além de alguns aprimoramentos adicionais.

## Tutoriais e laboratórios

- AWSLaboratório da Control Tower — Esses laboratórios fornecem uma visão geral de alto nível das tarefas comuns relacionadas à AWS Control Tower.
- No painel da AWS Control Tower, escolha Obter orientação personalizada se você tem um caso de uso em mente, mas não sabe por onde começar.
- Experimente visitar uma lista selecionada de YouTube vídeos que explicam mais sobre como usar a funcionalidade AWS Control Tower.

## Redes

Configure padrões repetíveis e gerenciáveis para redes em. AWS Saiba mais sobre design, automação e aparelhos que são comumente usados pelos clientes.

- AWS VPCArquitetura de início rápido — Este guia de início rápido fornece uma base de rede com base nas AWS melhores práticas para sua infraestrutura de AWS nuvem. Ele cria um AWS Virtual Private Network ambiente com sub-redes públicas e privadas onde você pode iniciar AWS serviços e outros recursos.
- Autoatendimento VPCs na AWS Control Tower usando o AWS Service Catalog — Esta postagem do blog descreve uma forma de configurar o Account Factory para que você possa provisionar contas com contas personalizadasVPCs.
- Implementação do Serverless Transit Network Orchestrator () na STNO Control Tower AWS — Esta postagem do blog demonstra como automatizar o acesso à conectividade de rede em todas as contas. Este blog é destinado aos administradores do AWS Control Tower ou aos responsáveis pelo gerenciamento de redes em seu AWS ambiente.

# Segurança, identidade e registro

Amplie sua postura de segurança, integre-se com provedores de identidade externos ou existentes e centralize os sistemas de registro.

Segurança

- Automatização de AWS Security Hub alertas com eventos do ciclo de vida da AWS Control Tower — Esta postagem do blog descreve como automatizar a ativação e a configuração do Security Hub em um ambiente de várias contas da Control AWS Tower em contas novas e existentes.
- Habilitando AWS Identity and Access Management — Esta postagem do blog descreve como aprimorar sua visibilidade de segurança organizacional habilitando e centralizando as descobertas do IAM Access Analyzer.
- AWSO Systems Manager Parameter Store fornece armazenamento seguro e hierárquico para gerenciamento de dados de configuração e gerenciamento de segredos. Você pode usá-lo para compartilhar informações de configuração em um local seguro, para uso pelo AWS Systems Manager e pelo AWS CloudFormation. Por exemplo, você pode armazenar uma lista de regiões nas quais deseja implantar pacotes de conformidade.

Identidade

- Vincule a identidade do usuário do Azure AD a AWS contas e aplicativos para login único — Esta postagem do blog descreve como usar o Azure AD com o IAM Identity Center e o AWS Control Tower.
- Gerencie o acesso AWS centralmente para usuários do Okta com AWS IAM Identity Center — Esta postagem do blog descreve como usar o Okta com o IAM Identity Center e o Control TowerAWS.

Registro em log

- AWS Solução de registro centralizado — Este post de soluções descreve a solução de registro centralizado, que permite que as organizações coletem, analisem e exibam registros AWS em várias contas e AWS regiões.

# Implantação de recursos e gerenciamento de cargas de trabalho

Implante e gerencie recursos e cargas de trabalho.

- Introdução à integração com a biblioteca — Esta postagem do blog descreve os portfólios de introdução que você pode usar.
- Implantação contínua do Cloud Custodian na Control Tower AWS

# Trabalhando com organizações e contas existentes

Trabalhe com AWS organizações e contas existentes.

- Inscrever uma conta — Este tópico do guia do usuário descreve como registrar uma AWS conta existente no AWS Control Tower.
- Traga uma conta para a AWS Control Tower — Esta postagem do blog descreve como implantar a AWS Control Tower em suas AWS organizações existentes.
- Estenda a governança da AWS Control Tower usando os pacotes de conformidade AWS Config — Esta postagem do blog descreve como implantar pacotes de AWS Config conformidade para ajudar a colocar contas e organizações existentes na governança pela Control Tower. AWS
- Como detectar e mitigar a violação do guardrail com o AWS Control Tower — Esta postagem do blog descreve como adicionar controles e como assinar SNS notificações para que você possa ser notificado por e-mail sobre violações de conformidade de controle.

# Automação e integração

Automatize a criação de contas e integre eventos do ciclo de vida com o Control TowerAWS.

- Eventos de ciclo de vida — Esta postagem do blog descreve como usar eventos de ciclo de vida com a Control Tower. AWS
- Automatize a criação de contas — Esta postagem do blog descreve como configurar a criação automática de contas no AWS Control Tower.
- Automação VPC de registros de fluxo da Amazon — Esta postagem do blog descreve como automatizar e centralizar os Amazon VPC Flow Logs em um ambiente com várias contas.

- Automatize a VPC marcação com eventos do ciclo de vida da AWS Control Tower — Esta postagem do blog descreve como automatizar a marcação de recursos por meio de eventos de ciclo de vida na Control Tower. VPCs AWS
- Gerenciamento automatizado de contas — Esta postagem do blog descreve como automatizar as tarefas de gerenciamento de contas após a configuração do ambiente AWS Control Tower.

## Migrar workloads

Use outros AWS serviços com o AWS Control Tower para auxiliar na migração da carga de trabalho.

- CloudEndure migração — Esta postagem do blog descreve como combinar CloudEndure e outros AWS serviços com o AWS Control Tower para auxiliar na migração da carga de trabalho.

## Serviços relacionados da AWS

AWSA Control Tower atua como uma camada de orquestração para. AWS Organizations Portanto, por meio do console AWS OrganizationsAPIs, você tem acesso a mais de 20 outros AWS serviços que funcionam com o AWS Control Tower. Esses serviços adicionais não podem ser acessados diretamente pelo console do AWS Control Tower.

- Para obter uma lista completa dos serviços disponíveis para a AWS Control Tower por meio do AWS Organizations, consulte AWSos serviços que você pode usar com o AWS Organizations.
- Para habilitar recursos de várias contas para esses AWS serviços relacionados, você deve habilitar o acesso confiável. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços.

  > **Note**
  >
  > Lembre-se de que o AWS IAM Identity Center AWS Config,, e AWS CloudTrail está configurado para você no AWS Control Tower e totalmente integrado. Você não precisa modificar suas configurações de acesso confiável ou administração delegada para esses serviços.

- Alguns AWS serviços disponíveis por meio do AWS Organizations podem usar administração delegada, incluindo o AWS Systems Manager e o AWS Firewall Manager. Para obter mais informações, consulte Configurando um administrador delegado e Habilitando uma conta de

administrador delegado para o Firewall Manager. Veja também este vídeo, Configurar grupos de segurança com o AWS Firewall Manager.

# AWS Marketplace soluções

Descubra soluções de AWS Marketplace.

- AWSControl Tower Marketplace — AWS Marketplace oferece uma ampla variedade de soluções para a AWS Control Tower para ajudá-lo a integrar software de terceiros. Essas soluções ajudam a resolver os principais casos de uso operacional e de infraestrutura, incluindo gerenciamento de identidade, segurança para um ambiente de várias contas, rede centralizada, inteligência operacional e gerenciamento de eventos e informações de segurança ()SIEM.

# AWSNotas de lançamento do Control Tower

As seções a seguir mostram detalhes sobre as versões da AWS Control Tower que exigem uma atualização para uma landing zone da AWS Control Tower, bem como as versões que são incorporadas automaticamente ao serviço.

Os recursos e lançamentos são listados em ordem cronológica inversa (os mais recentes primeiro) com base na data em que foram anunciados oficialmente ao público. Como pode haver um intervalo entre o momento em que o recurso ou lançamento é documentado e o momento em que é anunciado oficialmente, a data listada para um recurso ou lançamento aqui pode ser um pouco diferente da data noHistórico do documento.

Recursos lançados em 2024

Recursos lançados em 2023

Recursos lançados em 2022

Recursos lançados em 2021

Recursos lançados em 2020

Recursos lançados em 2019

## Janeiro de 2024 - presente

Desde janeiro de 2024, a AWS Control Tower lançou as seguintes atualizações:

- AWSO Control Tower suporta até 1.000 contas por UO
- AWSControl Tower adiciona seleção de versão de landing zone
- Controle descritivo API disponível, acesso expandido às regiões e controles
- AWSO Control Tower suporta AFT e o CFCT em regiões opcionais
- AWSO Control Tower adiciona o `ListLandingZoneOperations` API
- AWSO Control Tower suporta até 100 operações de controle simultâneas
- AWSControl Tower disponível em AWS Oeste do Canadá (Calgary)
- AWSA Control Tower suporta ajustes de cota de autoatendimento
- AWSA Control Tower lança o Guia de Referência de Controles

- AWSA Control Tower atualiza e renomeia dois controles proativos
- Controles obsoletos não estão mais disponíveis
- AWSO Control Tower suporta a marcação de `EnabledControl` recursos em AWS CloudFormation
- AWSO Control Tower suporta APIs registro e configuração de UO com linhas de base

## AWSO Control Tower suporta até 1.000 contas por UO

30 de agosto de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower aumentou o número máximo de contas permitidas por unidade organizacional (OU) de 300 para 1000. Agora, você pode inscrever até 1000 Contas da AWS na governança da AWS Control Tower de uma só vez, sem alterar sua estrutura de OU. Os processos de registro e novo registro da OU também são mais eficientes, exigindo muito menos tempo para implantar os recursos básicos da AWS Control Tower em suas contas.

Algumas limitações da conta ainda se aplicam devido às limitações no número de AWS CloudFormation conjuntos de pilhas disponíveis. Especificamente, o número máximo de contas que você pode inscrever em uma OU pode ser diferente, dependendo do número de regiões que você tem sob governança. Para saber mais, acesse Limitações com base no subjacente AWS serviços no Guia do usuário do AWS Control Tower. Para obter uma lista completa de Regiões da AWS onde AWS o Control Tower está disponível, consulte o Região da AWS Tabela.

## AWSControl Tower adiciona seleção de versão de landing zone

15 de agosto de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Se você estiver executando a versão 3.1 e superior da zona de pouso do AWS Control Tower, você pode atualizar ou reparar sua zona de pouso na versão atual, ou você pode atualizar para uma versão de sua escolha. Anteriormente, qualquer atualização ou reparo da zona de pouso exigia um upgrade para a versão mais recente da zona de pouso.

Com a seleção da versão do landing zone, você tem mais flexibilidade para planejar atualizações de versão enquanto avalia possíveis mudanças em seu ambiente. Você não precisa escolher entre reparar a deriva para manter a conformidade, atualizar as configurações da sua zona de pouso ou

atualizar para a versão mais recente da zona de pouso. Se você estiver executando a versão 3.1 ou superior da landing zone, você pode optar por permanecer na versão atual ou fazer o upgrade para uma versão mais nova ao atualizar ou redefinir as configurações da landing zone.

## Controle descritivo API disponível, acesso expandido às regiões e controles

6 de agosto de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower adicionou duas novas API operações que ajudam você a encontrar mais informações sobre os controles disponíveis de forma programática. Essa funcionalidade facilita a implantação de controles com automação.

- Ele `GetControl`APIretorna detalhes sobre um controle ativado, incluindo o identificador do alvo, um resumo das informações de controle, uma lista das regiões de destino e o status do desvio.
- `ListControls`APIRetorna uma lista paginada de todos os controles disponíveis na biblioteca de controles da AWS Control Tower.

Eles APIs são alcançados por meio do AWS Controle o namespace do catálogo. A ferramenta AWS O Control Catalog faz parte do AWS Control Tower, que inclui controles que ajudam você a gerenciar outros AWS serviços, não apenas AWS Control Tower. Esse catálogo expandido consolida controles de vários AWS serviços, para que você possa ver AWS controles de acordo com alguns casos de uso comuns, como: segurança, custo, durabilidade e operações. Para obter mais informações, consulte a API Referência do Catálogo de Controle.

Disponibilidade expandida da região

A partir desta versão, você pode estender a governança da AWS Control Tower para Regiões da AWS onde alguns de seus controles (já) habilitados não estão disponíveis. Além disso, agora você pode ativar determinados controles em mais regiões, mesmo que o controle não seja suportado em todas as suas regiões governadas.

Anteriormente, o AWS Control Tower impedia que você estendesse a governança às regiões ou habilitasse controles, quando não oferecia consistência em todos os seus controles habilitados e regiões governadas. Com esta versão, você tem mais flexibilidade e responsabilidade de garantir que sua configuração esteja correta para todos os controles habilitados e todas as regiões governadas. O AWScontrole Control Tower APIs e o catálogo de controle APIs podem ajudá-lo a obter informações sobre o AWS Regiões nas quais você está protegido por controles habilitados e

regiões nas quais controles adicionais podem ser implantados. As informações de região e controle também estão disponíveis no console AWS Control Tower.

## AWSO Control Tower suporta AFT e o CFCT em regiões opcionais

18 de julho de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Atualmente, as estruturas de personalização da AWS Control Tower Account Factory for Terraform (AFT) e Customizations for Control AWS Tower (cFct) estão disponíveis em mais cinco Regiões da AWS: Ásia-Pacífico (Hyderabad, Jacarta e Osaka), Israel (Tel Aviv) e Oriente Médio (). UAE

O Account Factory for Terraform (AFT) configura um pipeline do Terraform para ajudá-lo a provisionar e personalizar contas na AWS Control Tower. As personalizações do AWS Control Tower (CFCt) ajudam você a personalizar sua zona de pouso e suas contas da AWS Control Tower com AWS CloudFormation modelos e políticas de controle de serviços (SCPs).

Para saber mais, visite as páginas Account Factory for Terraform e Customizations for AWS Control Tower; no Control Tower User AWS Guide. Você também pode revisar as notas de lançamento na página do AFT Github e na página do cFct no Github. AFTe cFct são suportados em todos AWS Regiões, com algumas exceções. Para obter detalhes, consulte Limitações da região.

## AWSO Control Tower adiciona o **`ListLandingZoneOperations`** API

26 de junho de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower adicionou uma API que permite que você recupere uma lista das operações aplicadas recentemente à sua landing zone e das operações atualmente em andamento. Eles API podem retornar o histórico das operações da landing zone e seus identificadores por até 90 dias. Para exemplos de uso, consulte Exibir o status das operações do seu landing zone.

Para obter mais informações sobre o `ListLandingZoneOperations`API, consulte `ListLandingZoneOperations`na APIReferência da AWS Control Tower.

## AWSO Control Tower suporta até 100 operações de controle simultâneas

20 de maio de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora suporta várias operações de controle com maior simultaneidade. Você pode enviar até 100 operações de AWS controle da Control Tower, em várias unidades organizacionais (OUs), ao mesmo tempo, a partir do console ou comAPIs. Até dez (10) operações podem ser executadas simultaneamente, e as adicionais são colocadas em fila. Dessa forma, você pode definir uma configuração mais padronizada em vários Contas da AWS, sem a carga operacional das operações de controle repetitivas.

Para monitorar o status de suas operações de controle em andamento e em fila, você pode navegar até a nova página de operações recentes no console do AWS Control Tower ou pode chamar a nova. `ListControlOperations`API

A biblioteca AWS Control Tower contém mais de 500 controles, que são mapeados para diferentes objetivos de controle, estruturas e serviços. Para um objetivo de controle específico, como criptografar dados em repouso, você pode ativar vários controles com uma única operação de controle, para ajudá-lo a atingir o objetivo. Esse recurso facilita o desenvolvimento acelerado, permite a adoção mais rápida dos controles de melhores práticas e reduz as complexidades operacionais.

## AWSControl Tower disponível em AWS Oeste do Canadá (Calgary)

3 de maio de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

A partir de hoje, você pode ativar a AWS Control Tower na região Oeste do Canadá (Calgary). Se você já implantou a AWS Control Tower e deseja estender seus recursos de governança para essa região, pode fazer isso com a landing zone APIs da AWS Control Tower. Ou, no console, acesse a página Configurações no painel do AWS Control Tower, selecione suas regiões e atualize sua landing zone.

A região Oeste do Canadá (Calgary) não oferece suporte AWS Service Catalog. Por esse motivo, algumas funcionalidades do AWS Control Tower são diferentes. A mudança de funcionalidade mais notável é que o Account Factory não está disponível. Se você escolher o Oeste do Canadá (Calgary) como sua região de origem, os procedimentos para atualizar contas, configurar automações de contas e quaisquer outros processos que envolvam o Service Catalog serão diferentes dos de outras regiões.

Provisionamento de contas

Para criar e provisionar uma nova conta na região Oeste do Canadá (Calgary), recomendamos que você crie uma conta fora da AWS Control Tower e, em seguida, inscreva-a em uma OU registrada.

Para obter mais informações, consulte Inscrever uma conta existente e Etapas para registrar uma conta.

O Service Catalog não APIs está disponível na região Oeste do Canadá (Calgary). O script de exemplo mostrado em Automatizar o provisionamento de contas no AWS Control Tower by Service Catalog não APIs é viável.

Account Factory Customizations (AFC), Account Factory for Terraform (AFT) e Customizations for Control AWS Tower (CFCt) não estão disponíveis no Oeste do Canadá (Calgary), devido à falta de outras dependências subjacentes para a Control Tower. AWS Se você estender a governança para a região Oeste do Canadá (Calgary), poderá continuar gerenciando os AFC blueprints em todas as regiões que a AWS Control Tower oferece suporte, desde que o Service Catalog esteja disponível em sua região de origem.

Controles

Controles e controles proativos para o AWS Security Hub Service-Managed Standard: AWS Control Tower não  está disponível na região Oeste do Canadá (Calgary). O controle preventivo não `CT.CLOUDFORMATION.PR.1` está disponível no Oeste do Canadá (Calgary) porque é necessário apenas para ativar os controles proativos baseados em ganchos. Certos controles de detetive baseados em AWS Config não estão disponíveis. Para obter detalhes, consulte Limitações de controle.

Provedor de identidade

IAMO Identity Center não está disponível no Oeste do Canadá (Calgary). A recomendação de melhores práticas é configurar seu landing zone em uma região onde o IAM Identity Center esteja disponível. Como alternativa, você tem a opção de autogerenciar sua configuração de acesso à conta se usar um provedor de identidade externo no Oeste do Canadá (Calgary).

A indisponibilidade do Service Catalog na região Oeste do Canadá (Calgary) não tem efeito em outras regiões que são suportadas pela AWS Control Tower. Essas diferenças se aplicam somente se sua região de origem for o Oeste do Canadá (Calgary).

Para obter uma lista completa das regiões em que o AWS Control Tower está disponível, consulte o AWS Tabela de regiões.

## AWSA Control Tower suporta ajustes de cota de autoatendimento

25 de abril de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora oferece suporte a ajustes de cotas de autoatendimento por meio do console Service Quotas. Para obter mais informações, consulte Solicitar um aumento da cota.

## AWSA Control Tower lança o Guia de Referência de Controles

21 de abril de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower lançou o Controls Reference Guide, um novo documento no qual você pode encontrar informações detalhadas sobre os controles específicos do ambiente da AWS Control Tower. Anteriormente, esse material estava incluído no Guia do Usuário do AWS Control Tower. O Guia de referência de controles abrange os controles em um formato expandido. Para obter mais informações, consulte o Guia de referência dos controles da AWS Control Tower.

## AWSA Control Tower atualiza e renomeia dois controles proativos

26 de março de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower renomeou dois controles proativos para se alinharem às atualizações do Amazon Service. OpenSearch

- [CT.OPENSEARCH.PR.8] Exigir um domínio do Elasticsearch Service para usar .2 TLSv1
- [CT.OPENSEARCH.PR.16 ] Exigir um domínio OpenSearch do Amazon Service para usar TLSv1 .2

Atualizamos os nomes dos controles e os artefatos desses dois controles para se alinharem à versão recente do Amazon OpenSearch Service, que agora oferece suporte à versão 1.3 do Transport Layer Security (TLS) entre suas opções de segurança de transporte para segurança de endpoints de domínio.

Para adicionar suporte para TLSv1 .3 para esses controles, atualizamos o artefato e o nome dos controles para refletir a intenção do controle. Agora, eles avaliam a TLS versão mínima do domínio do serviço. Para fazer essa atualização em seu ambiente, você deve desativar e ativar os controles para implantar o artefato mais recente.

Nenhum outro controle proativo é afetado por essa alteração. Recomendamos que você revise esses controles para garantir que eles atendam aos seus objetivos de controle.

Em caso de dúvidas ou preocupações, entre em contato AWS Support.

## Controles obsoletos não estão mais disponíveis

12 de março de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower descontinuou alguns controles. Esses controles não estão mais disponíveis.

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

## AWSO Control Tower suporta a marcação de **`EnabledControl`** recursos em AWS CloudFormation

22 de fevereiro de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Esta versão do AWS Control Tower atualiza o comportamento do `EnabledControl` recurso, para se alinhar melhor aos controles configuráveis e melhorar a capacidade de gerenciar seu ambiente de AWS Control Tower com automação. Com esta versão, você pode adicionar tags aos `EnabledControl` recursos configuráveis por meio de AWS CloudFormation modelos. Anteriormente, era possível adicionar tags APIs somente por meio do console AWS Control Tower.

As `ListTagsforResource` API operações da AWS Control Tower `GetEnabledControlEnableControl`,, e são atualizadas com esta versão porque dependem da funcionalidade do `EnabledControl` recurso.

Para obter mais informações, consulte Marcar `EnabledControl` recursos no AWS Control Tower e `EnabledControl`no AWS CloudFormation Guia do usuário.

## AWSO Control Tower suporta APIs registro e configuração de UO com linhas de base

14 de fevereiro de 2024

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Eles APIs oferecem suporte ao registro programático de OU com a `EnableBaseline` chamada. Quando você habilita uma linha de base em uma OU, as contas dos membros dentro da OU são inscritas na governança da AWS Control Tower. Algumas ressalvas podem ser aplicadas. Por exemplo, o registro de UO por meio do console AWS Control Tower permite controles opcionais, bem como controles obrigatórios. Ao ligarAPIs, talvez seja necessário concluir uma etapa extra para que os controles opcionais sejam ativados.

Uma linha de base da AWS Control Tower incorpora as melhores práticas para a governança da AWS Control Tower de uma OU e contas de membros. Por exemplo, quando você habilita uma linha de base em uma OU, as contas de membros dentro da OU recebem um grupo definido de recursos, incluindo AWS CloudTrail, AWS Config, IAM Identity Center e obrigatório AWS IAMpapéis.

Linhas de base específicas são compatíveis com versões específicas da zona de pouso do AWS Control Tower. AWSA Control Tower pode aplicar a linha de base compatível mais recente à sua zona de pouso quando você altera as configurações da zona de pouso. Para obter mais informações, consulte Compatibilidade das linhas de base da OU e das versões do landing zone.

Esta versão inclui quatro itens essenciais Tipos de linhas de base

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Com as linhas de base novas APIs e definidas, você pode registrar OUs e automatizar seu fluxo de trabalho de provisionamento de OU. Eles APIs também podem gerenciar o OUs que já está sob a governança da AWS Control Tower, para que você possa se registrar novamente OUs

após as atualizações da landing zone. Eles APIs incluem suporte para um AWS CloudFormation `EnabledBaseline`recurso, que permite gerenciar sua OUs infraestrutura como código (IaC).

Linha de base APIs

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Aja com base em uma linha de base para uma OU.
- GetEnabledBaseline, ListEnabledBaselines: Descubra as configurações para suas linhas de base habilitadas.
- GetBaselineOperation: Visualize o status de uma operação de linha de base específica.
- ResetEnabledBaseline: corrija o desvio de recursos em uma OU com uma linha de base habilitada (incluindo desvio de controle aninhado OUs e obrigatório). Também corrige a deriva para a landing-zone-level Região, negar o controle.
- GetBaseline, ListBaselines: Descubra o conteúdo das linhas de base da AWS Control Tower.

Para saber mais sobre elasAPIs, consulte as linhas de base no Guia do usuário do AWS Control Tower e na API Referência. Os novos APIs estão disponíveis em Regiões da AWS onde a AWS Control Tower está disponível, exceto nas regiões GovCloud (EUA). Para uma lista de Regiões da AWS onde AWS o Control Tower está disponível, consulte o Região da AWS Tabela.

## Janeiro - dezembro de 2023

Em 2023, a AWS Control Tower lançou as seguintes atualizações:

- Transição para um novo AWS Service Catalog Tipo de produto externo (fase 3)
- AWSVersão 3.3 da zona de pouso da Control Tower
- Transição para um novo AWS Service Catalog Tipo de produto externo (fase 2)
- AWSControl Tower anuncia controles para auxiliar a soberania digital
- AWSControl Tower suporta landing zone APIs
- AWSO Control Tower suporta marcação para controles habilitados
- AWSControl Tower disponível na região Ásia-Pacífico (Melbourne)
- Transição para um novo AWS Service Catalog Tipo de produto externo (fase 1)
- Novo controle API disponível

- AWSControl Tower adiciona controles adicionais
- Novo tipo de desvio relatado: acesso confiável desativado
- Quatro adicionais Regiões da AWS
- AWSControl Tower disponível na região de Tel Aviv
- AWSControl Tower lança 28 novos controles proativos
- AWSA Control Tower suspende o uso de dois controles
- AWSVersão 3.2 da zona de pouso da Control Tower
- AWSA Control Tower gerencia contas com base em ID
- Controles de detetive adicionais do Security Hub disponíveis na biblioteca de controles da AWS Control Tower
- AWSA Control Tower publica tabelas de metadados de controle
- Suporte do Terraform para Account Factory Customization
- AWS IAMAutogerenciamento do Identity Center disponível para landing zone
- AWSControl Tower aborda a governança mista para OUs
- Controles proativos adicionais disponíveis
- Controles EC2 proativos atualizados da Amazon
- Sete adicionais Regiões da AWS available
- Account Factory para rastreamento de solicitações de personalização de conta do Terraform (AFT)
- AWSVersão 3.1 da zona de pouso da Control Tower
- Controles proativos geralmente disponíveis

## Transição para um novo AWS Service Catalog Tipo de produto externo (fase 3)

14 de dezembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower não oferece mais suporte ao Terraform Open Source como um tipo de produto (blueprint) ao criar um novo Contas da AWS. Para obter mais informações e instruções sobre como

atualizar os esquemas da sua conta, consulte Transição para o AWS Service Catalog Tipo de produto externo.

Se você não atualizar seus blueprints de conta para usar o tipo de produto externo, você só poderá atualizar ou encerrar contas que você provisionou usando blueprints de código aberto do Terraform.

## AWSVersão 3.3 da zona de pouso da Control Tower

14 de dezembro de 2023

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 3.3. Para obter informações, consulteAtualize sua landing zone).

Atualizações na política de bucket do S3 na conta do AWS Control Tower Audit

Modificamos a política de bucket de auditoria do Amazon S3 que a AWS Control Tower implanta nas contas, de modo que uma `aws:SourceOrgID` condição deve ser atendida para qualquer permissão de gravação. Com esta versão, AWS os serviços têm acesso aos seus recursos somente quando a solicitação é originada de sua organização ou unidade organizacional (OU).

Você pode usar a chave de `aws:SourceOrgID` condição e definir o valor do ID da sua organização no elemento de condição da sua política de bucket do S3. Essa condição garante que CloudTrail somente registros em nome de contas dentro de sua organização possam ser gravados em seu bucket do S3; ela impede que CloudTrail registros de fora da sua organização gravem em seu bucket do AWS Control Tower S3.

Fizemos essa alteração para corrigir uma possível vulnerabilidade de segurança, sem afetar a funcionalidade de suas cargas de trabalho existentes. Para ver a política atualizada, consultePolítica de bucket do Amazon S3 na conta de auditoria.

Para obter mais informações sobre a nova chave de condição, consulte a IAM documentação e a postagem do IAM blog intitulada "Use controles escaláveis para AWS serviços acessando seus recursos.”

Atualizações da política no AWS Config SNStópico

Adicionamos a nova chave de `aws:SourceOrgID` condição à política do AWS Config SNSTópico. Para ver a política atualizada, consulte O AWS Config SNSpolítica de tópicos.

Atualizações no controle Region Deny da zona de pouso

- Removido`discovery-marketplace:`. Esta ação é coberta pela `aws-marketplace:*` isenção.

- `quicksight:DescribeAccountSubscription` adicionado

Atualizado AWS CloudFormation modelo

Nós atualizamos o AWS CloudFormation modelo para a pilha chamada de `BASELINE-CLOUDTRAIL-MASTER` forma que não mostre deriva quando AWS KMS a criptografia não é usada.

## Transição para um novo AWS Service Catalog Tipo de produto externo (fase 2)

7 de dezembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

HashiCorp atualizou seu licenciamento do Terraform. Como resultado, AWS Service Catalog alterou o suporte para produtos Terraform Open Source e produtos provisionados para um novo tipo de produto, chamado Externo.

Para evitar interrupções nas cargas de trabalho existentes e AWS recursos em suas contas, siga as etapas de transição da AWS Control Tower em Transition to the AWS Service Catalog Tipo de produto externo até 14 de dezembro de 2023.

## AWSControl Tower anuncia controles para auxiliar a soberania digital

27 de novembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSControl Tower anuncia 65 novos AWS-controles gerenciados, para ajudá-lo a atender aos seus requisitos de soberania digital. Com esta versão, você pode descobrir esses controles sob um novo grupo de soberania digital no console AWS Control Tower. Você pode usar esses controles para ajudar a evitar ações e detectar alterações de recursos em relação à residência de dados, restrição de acesso granular, criptografia e recursos de resiliência. Esses controles foram projetados para simplificar o atendimento dos requisitos em grande escala. Para obter mais informações sobre controles de soberania digital, consulte Controles que aprimoram a proteção da soberania digital.

Por exemplo, você pode optar por ativar controles que ajudem a aplicar suas estratégias de criptografia e resiliência, como  Exigir um AWS AppSync APIcache para ter a criptografia em trânsito habilitada  ou  exigir um AWS Firewall de rede a ser implantado em várias zonas  de disponibilidade.

Você também pode personalizar o AWS controle de negação da região da Control Tower para aplicar restrições regionais que melhor atendam às suas necessidades comerciais exclusivas.

Esta versão traz recursos bem aprimorados de negação da AWS Control Tower Region. Você pode aplicar um novo controle parametrizado de negação de região no nível da OU, para aumentar a granularidade da governança e, ao mesmo tempo, manter a governança adicional da região no nível da landing zone. Esse controle de negação de região personalizável ajuda você a aplicar restrições regionais que melhor atendam às suas necessidades comerciais exclusivas. Para obter mais informações sobre o novo controle de negação de região configurável, consulte Controle de negação de região aplicado à OU.

Como uma nova ferramenta para o novo aprimoramento de negação de região, esta versão inclui uma nova API`UpdateEnabledControl`,, que permite redefinir seus controles ativados para as configurações padrão. Isso API é especialmente útil em casos de uso em que você precisa resolver o desvio rapidamente ou para garantir programaticamente que um controle não esteja em um estado de desvio. Para obter mais informações sobre o novoAPI, consulte a API Referência da AWS Control Tower

Novos controles proativos

- CT.APIGATEWAY.PR.6: Exija que um REST domínio do Amazon API Gateway use uma política de segurança que especifique uma versão mínima do TLS protocolo de TLSv1 2.
- CT.APPSYNC.PR.2: Exigir um AWS AppSync GraphQL API a ser configurado com visibilidade privada
- CT.APPSYNC.PR.3: Exigir que um AWS AppSync O GraphQL não API é autenticado com chaves API
- CT.APPSYNC.PR.4: Exigir um AWS AppSync APICache do GraphQL para ter a criptografia em trânsito ativada.
- CT.APPSYNC.PR.5: Exigir um AWS AppSync APICache do GraphQL para ter a criptografia em repouso ativada.
- CT.AUTOSCALING.PR.9: Exija um EBS volume da Amazon configurado por meio de uma configuração de lançamento do Amazon EC2 Auto Scaling para criptografar dados em repouso
- CT.AUTOSCALING.PR.10: Exija que um grupo do Amazon EC2 Auto Scaling use somente AWS Tipos de instância Nitro ao substituir um modelo de execução
- CT.AUTOSCALING.PR.11: Exigir somente AWS Tipos de instância Nitro que oferecem suporte à criptografia de tráfego de rede entre instâncias a serem adicionadas a um grupo do Amazon EC2 Auto Scaling, ao substituir um modelo de execução

- CT.DAX.PR.3: Exigir um cluster do DynamoDB Accelerator para criptografar dados em trânsito com o Transport Layer Security () TLS
- CT.DMS.PR.2: Exigir um AWS Endpoint do Database Migration Service (DMS) para criptografar conexões para endpoints de origem e destino
- CT.EC2.PR.15: Exigir uma EC2 instância da Amazon para usar um AWS Tipo de instância Nitro ao criar a partir do tipo de `AWS::EC2::LaunchTemplate` recurso
- CT.EC2.PR.16: Exigir uma EC2 instância da Amazon para usar um AWS Tipo de instância Nitro quando criada usando o tipo `AWS::EC2::Instance` de recurso
- CT.EC2.PR.17: Exigir que um host EC2 dedicado da Amazon use um tipo de instância AWS Nitro
- CT.EC2.PR.18: Exija que uma EC2 frota da Amazon substitua somente os modelos de lançamento com AWS Tipos de instância Nitro
- CT.EC2.PR.19: Exija que uma EC2 instância da Amazon use um tipo de instância nitro que ofereça suporte à criptografia em trânsito entre instâncias quando criada usando o `AWS::EC2::Instance` tipo de recurso
- CT.EC2.PR.20: Exija que uma EC2 frota da Amazon substitua somente os modelos de lançamento com AWS Tipos de instância Nitro que oferecem suporte à criptografia em trânsito entre instâncias
- CT.ELASTICACHE.PR.8: Exija que um grupo de ElastiCache replicação da Amazon de versões posteriores do Redis tenha RBAC a autenticação ativada
- CT.MQ.PR.1: Exija que um agente Amazon MQ ActiveMQ use o modo de implantação ativo/em espera para alta disponibilidade
- CT.MQ.PR.2: Exija que um agente Amazon MQ Rabbit MQ use o modo de cluster Multi-AZ para alta disponibilidade
- CT.MSK.PR.1: Exija um cluster Amazon Managed Streaming for Apache MSK Kafka () para aplicar a criptografia em trânsito entre os nós do cluster broker
- CT.MSK.PR.2: Exija que um cluster Amazon Managed Streaming for Apache MSK Kafka () seja configurado com desativado PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Exigir um AWS Firewall de rede: firewall a ser implantado em várias zonas de disponibilidade
- CT.RDS.PR.26: Exigir um Amazon RDS DB Proxy para exigir conexões Transport Layer Security (TLS)
- CT.RDS.PR.27: Exigir um grupo de parâmetros de RDS cluster de banco de dados da Amazon para exigir conexões Transport Layer Security (TLS) para tipos de mecanismos compatíveis

- CT.RDS.PR.28: Exigir um grupo de parâmetros do Amazon RDS DB para exigir conexões Transport Layer Security (TLS) para tipos de mecanismos compatíveis
- CT.RDS.PR.29: Exija que um RDS cluster da Amazon não seja configurado para ser acessível publicamente por meio da propriedade PubliclyAccessible "
- CT.RDS.PR.30: Exija que uma instância RDS de banco de dados da Amazon tenha criptografia em repouso configurada para usar uma KMS chave que você especifique para os tipos de mecanismos compatíveis
- CT.S3.PR.12: Exija que um ponto de acesso Amazon S3 tenha uma configuração Block Public Access (BPA) com todas as opções definidas como verdadeiras

Novos controles preventivos

- CT.APPSYNC.PV.1 Exigir que um AWS AppSync O GraphQL API é configurado com visibilidade privada
- CT.EC2.PV.1 Exija que um EBS snapshot da Amazon seja criado a partir de um volume criptografado EC2
- CT.EC2.PV.2 Exija que um EBS volume anexado da Amazon esteja configurado para criptografar dados em repouso
- CT.EC2.PV.3 Exija que um EBS snapshot da Amazon não possa ser restaurado publicamente
- CT.EC2.PV.4 Exija que o Amazon EBS Direct APIs não seja chamado
- CT.EC2.PV.5 Proibir o uso da importação e exportação da Amazon EC2 VM
- CT.EC2.PV.6 Proibir o uso de Amazon e ações obsoletas EC2 RequestSpotFleet RequestSpotInstances API
- CT.KMS.PV.1 Exigir um AWS KMS política fundamental para ter uma declaração que limite a criação de AWS KMS subsídios para AWS serviços
- CT.KMS.PV.2 Exigir que um AWS KMS chave assimétrica com material de RSA chave usado para criptografia não tem um comprimento de chave de 2048 bits
- CT.KMS.PV.3 Exigir que um AWS KMS a chave está configurada com a verificação de segurança de bloqueio de política de desvio ativada
- CT.KMS.PV.4 Exigir que um AWS KMS a chave gerenciada pelo cliente (CMK) é configurada com material de chave proveniente de AWS Nuvem HSM
- CT.KMS.PV.5 Exigir que um AWS KMS a chave gerenciada pelo cliente (CMK) é configurada com material de chave importado

- CT.KMS.PV.6 Exigir que um AWS KMS a chave gerenciada pelo cliente (CMK) é configurada com material de chave proveniente de um armazenamento de chaves externo () XKS
- CT.LAMBDA.PV.1 Exigir um AWS Lambda função URL a ser usada AWS IAMautenticação baseada
- CT.LAMBDA.PV.2 Exigir um AWS Lambda função URL a ser configurada para acesso somente por diretores dentro de seu Conta da AWS
- CT. MULTISERVICE.PV.1: negar acesso a AWS com base no solicitado Região da AWS para uma unidade organizacional

Os novos controles de detetives que aprimoram sua postura de governança de soberania digital fazem parte do AWS Security Hub AWSControl Tower padrão gerenciado por serviços.

Novos controles de detetive

- SH.ACM.2: RSA os certificados gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- SH.AppSync.5: AWS AppSync O GraphQL não APIs deve ser autenticado com chaves API
- SH.CloudTrail.6: certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público:
- SH.DMS.9: os DMS endpoints devem usar SSL
- SH.DocumentDB.3: Os snapshots manuais do cluster do Amazon DocumentDB não devem ser públicos
- SH.DynamoDB.3: os clusters do DynamoDB Accelerator DAX () devem ser criptografados em repouso
- SH.EC2.23: Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de VPC anexos
- SH.EKS.1: os endpoints do EKS cluster não devem ser acessíveis ao público
- SH.ElastiCache.3: os grupos ElastiCache de replicação devem ter o failover automático ativado
- SH.ElastiCache.4: os grupos ElastiCache de replicação deveriam estar habilitados encryption-at-rest
- SH.ElastiCache.5: os grupos ElastiCache de replicação deveriam estar habilitados encryption-in-transit
- SH.ElastiCache.6: grupos ElastiCache de replicação de versões anteriores do Redis devem ter o Redis ativado AUTH

- SH.EventBridge.3: os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- SH.KMS.4: AWS KMS a rotação de chaves deve ser ativada
- SH.Lambda.3: As funções Lambda devem estar em um VPC
- SH.MQ.5: Os corretores ActiveMQ devem usar o modo de implantação ativo/em espera
- SH.MQ.6: os corretores RabbitMQ devem usar o modo de implantação de cluster
- SH.MSK.1: MSK os clusters devem ser criptografados em trânsito entre os nós do corretor
- SH.RDS.12: a IAM autenticação deve ser configurada para RDS clusters
- SH.RDS.15: clusters de RDS banco de dados devem ser configurados para várias zonas de disponibilidade
- SH.S3.17: os buckets S3 devem ser criptografados em repouso com AWS KMS keys

Para obter mais informações sobre os controles adicionados ao AWS Security Hub Torre de AWS controle padrão gerenciada por serviços, consulte Controles que se aplicam ao padrão gerenciado por serviços: Control Tower AWS no AWS Security Hub documentação.

Para uma lista de Regiões da AWS que não suportam determinados controles que fazem parte do AWS Security Hub AWSControl Tower padrão gerenciado por serviços, consulte Regiões não suportadas.

Novo controle configurável para negação de região no nível da OU

CT. MULTISERVICE.PV.1: Esse controle aceita parâmetros para especificar regiões, IAM diretores e ações isentas que são permitidas, no nível da OU, em vez de para toda a landing zone da Control Tower. AWS É um controle preventivo, implementado pela política de controle de serviços (SCP).

Para obter mais informações, consulte Controle de negação de região aplicado à OU.

O **`UpdateEnabledControl`** API

Esta versão do AWS Control Tower adiciona o seguinte API suporte para controles:

- O atualizado `EnableControl` API pode configurar controles que são configuráveis.
- A atualização `GetEnabledControl` API mostra os parâmetros configurados em um controle ativado.
- O novo `UpdateEnabledControl` API pode alterar os parâmetros em um controle ativado.

Para obter mais informações, consulte a APIReferência da AWS Control Tower.

## AWSControl Tower suporta landing zone APIs

26 de novembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora suporta a configuração da landing zone e o uso do lançamentoAPIs. Você pode criar, atualizar, obter, listar, redefinir e excluir zonas de pouso usandoAPIs.

O seguinte APIs permite que você configure e gerencie sua landing zone programaticamente usando AWS CloudFormation ou o AWS CLI.

AWSO Control Tower suporta o seguinte APIs para zonas de pouso:

- `CreateLandingZone`—Essa API chamada cria uma zona de pouso usando uma versão da zona de pouso e um arquivo de manifesto.
- `GetLandingZoneOperation`—Essa API chamada retorna o status de uma operação de landing zone especificada.
- `GetLandingZone`—Essa API chamada retorna detalhes sobre a landing zone especificada, incluindo a versão, o arquivo de manifesto e o status.
- `UpdateLandingZone`—Essa API chamada atualiza a versão do landing zone ou o arquivo de manifesto.
- `ListLandingZone`—Essa API chamada retorna um identificador de zona de pouso (ARN) para uma configuração de zona de pouso na conta de gerenciamento.
- `ResetLandingZone`—Essa API chamada redefine o landing zone para os parâmetros especificados na atualização mais recente, o que pode reparar a deriva. Se a zona de pouso não tiver sido atualizada, essa chamada redefinirá a zona de pouso para os parâmetros especificados na criação.
- `DeleteLandingZone`—Essa API chamada desativa a landing zone.

Para começar a usar o landing zoneAPIs, veja Comece a usar o AWS Control Tower usando APIs o.

## AWSO Control Tower suporta marcação para controles habilitados

10 de novembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora suporta a marcação de recursos para controles habilitados, a partir do console da AWS Control Tower ou por meio deAPIs. Você pode adicionar, remover ou listar tags para os controles ativados.

Com a versão a seguirAPIs, você pode configurar tags para os controles ativados no AWS Control Tower. As tags ajudam a gerenciar, identificar, organizar, pesquisar e filtrar recursos. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios.

AWSO Control Tower suporta o seguinte APIs para marcação de controle:

- `TagResource`—Essa API chamada adiciona tags aos controles ativados na AWS Control Tower.
- `UntagResource`—Essa API chamada remove as tags dos controles ativados no AWS Control Tower.
- `ListTagsForResource`—Essa API chamada retorna tags para controles habilitados no AWS Control Tower.

AWSOs controles da Control Tower APIs estão disponíveis em Regiões da AWS onde a AWS Control Tower está disponível. Para obter uma lista completa de Regiões da AWS em que o AWS Control Tower está disponível, consulte o AWS Tabela de regiões. Para obter uma lista completa do AWS Control TowerAPIs, consulte a APIReferência.

## AWSControl Tower disponível na região Ásia-Pacífico (Melbourne)

3 de novembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower está disponível na região Ásia-Pacífico (Melbourne).

Se você já estiver usando o AWS Control Tower e quiser estender seus recursos de governança para essa região em suas contas, acesse a página Configurações no painel da AWS Control Tower, selecione a Região e atualize sua landing zone. Depois de atualizar a landing zone, você deve atualizar todas as contas que são administradas pela AWS Control Tower para colocar suas contas OUs sob controle na nova região. Para obter mais informações, consulte Sobre atualizações.

Para obter uma lista completa das regiões nas quais o AWS Control Tower está disponível, consulte o Região da AWS Tabela.

## Transição para um novo AWS Service Catalog Tipo de produto externo (fase 1)

31 de outubro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

HashiCorp atualizou seu licenciamento do Terraform. Como resultado, AWS Service Catalog suporte atualizado para produtos Terraform Open Source e produtos provisionados para um novo tipo de produto, chamado Externo.

AWSO Control Tower não oferece suporte às personalizações do Account Factory que dependem do AWS Service Catalog Tipo de produto externo. Para evitar interrupções nas cargas de trabalho existentes e AWS recursos em suas contas, siga as etapas de transição do AWS Control Tower na ordem sugerida, até 14 de dezembro de 2023:

1. Atualize seu Terraform Reference Engine existente para AWS Service Catalog para incluir suporte para os tipos de produtos externos e de código aberto do Terraform. Para obter instruções sobre como atualizar seu Terraform Reference Engine, consulte o AWS Service Catalog GitHub Repositório.
2. Acesse AWS Service Catalog e duplique qualquer projeto existente do Terraform Open Source para usar o novo tipo de produto externo. Não encerre os blueprints existentes do Terraform Open Source.
3. Continue usando seus blueprints existentes do Terraform Open Source para criar ou atualizar contas na AWS Control Tower.

## Novo controle API disponível

14 de outubro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora oferece suporte a um adicional API que você pode usar para implantar e gerenciar seus controles da AWS Control Tower, em grande escala. Para obter mais informações sobre o AWS controle Control TowerAPIs, consulte a APIReferência.

AWSA Control Tower adicionou um novo controleAPI.

- `GetEnabledControl`— A API chamada fornece detalhes sobre um controle ativado.

Também atualizamos issoAPI:

`ListEnabledControls`—Essa API chamada lista os controles ativados pelo AWS Control Tower na unidade organizacional especificada e as contas que ela contém. Agora, ele retorna informações adicionais em um `EnabledControlSummary` objeto.

Com elesAPIs, você pode realizar várias operações comuns de forma programática. Por exemplo:

- Obtenha uma lista de todos os controles que você ativou na biblioteca de controles da AWS Control Tower.
- Para qualquer controle ativado, você pode obter informações sobre as regiões nas quais o controle é suportado, o identificador do controle (ARN), o status de desvio do controle e o resumo do status do controle.

AWSOs controles da Control Tower APIs estão disponíveis em Regiões da AWS onde a AWS Control Tower está disponível. Para obter uma lista completa de Regiões da AWS em que o AWS Control Tower está disponível, consulte o AWS Tabela de regiões. Para obter uma lista completa do AWS Control TowerAPIs, consulte a APIReferência.

## AWSControl Tower adiciona controles adicionais

5 de outubro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower anuncia novos controles proativos e de detetive.

Os controles proativos no AWS Control Tower são implementados por meio de AWS CloudFormation Ganchos, que identificam e bloqueiam recursos não compatíveis antes AWS CloudFormation os provisiona. Os controles proativos complementam os recursos de controle preventivo e de detetive existentes no AWS Control Tower.

Novos controles proativos

- [CT.ATHENA.PR.1] Exija que um grupo de trabalho do Amazon Athena criptografe os resultados da consulta do Athena em repouso
- [CT.ATHENA.PR.2] Exija que um grupo de trabalho do Amazon Athena criptografe os resultados da consulta do Athena em repouso com um AWS Key Management Service (KMS) chave
- [CT.CLOUDTRAIL.PR.4] Exigir um AWS CloudTrail Armazenamento de dados de eventos Lake para permitir a criptografia em repouso com um AWS KMS chave

- [CT.DAX.PR.2] Exigir um DAX cluster da Amazon para implantar nós em pelo menos três zonas de disponibilidade
- [CT.EC2.PR.14] Exigir um EBS volume da Amazon configurado por meio de um modelo de EC2 lançamento da Amazon para criptografar dados em repouso
- [CT.EKS.PR.2] Exija que um EKS cluster da Amazon seja configurado com criptografia secreta usando AWS Chaves do Serviço de Gerenciamento de Chaves (KMS)
- [CT.ELASTICLOADBALANCING.PR.14] Exigir que um Network Load Balancer tenha o balanceamento de carga entre zonas ativado
- [CT.ELASTICLOADBALANCING.PR.15] Exija que um grupo-alvo do Elastic Load Balancing v2 não desabilite explicitamente o balanceamento de carga entre zonas
- [CT.EMR.PR.1] Exija que uma configuração de segurança Amazon EMR (EMR) esteja configurada para criptografar dados em repouso no Amazon S3
- [CT.EMR.PR.2] Exija que uma configuração de segurança Amazon EMR (EMR) esteja configurada para criptografar dados em repouso no Amazon S3 com um AWS KMS chave
- [CT.EMR.PR.3] Exija que uma configuração de segurança da Amazon EMR (EMR) seja configurada com criptografia de disco local de EBS volume usando um AWS KMS chave
- [CT.EMR.PR.4] Exija que uma configuração de segurança da Amazon EMR (EMR) esteja configurada para criptografar dados em trânsito
- [CT.GLUE.PR.1] Exigir um AWS Glue o trabalho para ter uma configuração de segurança associada
- [CT.GLUE.PR.2] Exigir um AWS Glue a configuração de segurança para criptografar dados em destinos do Amazon S3 usando AWS KMSchaves
- [CT.KMS.PR.2] Exigir que um AWS KMS chave assimétrica com material de RSA chave usado para criptografia tem um comprimento de chave maior que 2048 bits
- [CT.KMS.PR.3] Exigir um AWS KMS política fundamental para ter uma declaração que limite a criação de AWS KMS subsídios para AWS serviços
- [CT.LAMBDA.PR.4] Exigir um AWS Lambda permissão de camada para conceder acesso a um AWS organização ou específica AWS conta
- [CT.LAMBDA.PR.5] Exigir um AWS Lambda função URL a ser usada AWS IAMautenticação baseada
- [CT.LAMBDA.PR.6] Exigir um AWS Lambda URLCORSpolítica de funções para restringir o acesso a origens específicas

- [CT.NEPTUNE.PR.4] Exija um cluster de banco de dados Amazon Neptune para permitir a exportação de logs da CloudWatch Amazon para registros de auditoria
- [CT.NEPTUNE.PR.5] Exija um cluster de banco de dados Amazon Neptune para definir um período de retenção de backup maior ou igual a sete dias
- [CT.REDSHIFT.PR.9] Exija que um grupo de parâmetros de cluster do Amazon Redshift esteja configurado para usar o Secure Sockets Layer (SSL) para criptografia de dados em trânsito

Esses novos controles proativos estão disponíveis no mercado Regiões da AWS onde a AWS Control Tower está disponível. Para obter mais detalhes sobre esses controles, consulte Controles proativos. Para obter mais detalhes sobre onde os controles estão disponíveis, consulte Limitações de controle.

Novos controles de detetive

Novos controles foram adicionados ao Padrão Gerenciado de Serviços do Security Hub: AWS Control Tower. Esses controles ajudam você a aprimorar sua postura de governança. Eles agem como parte do Security Hub Service-Managed Standard: AWS Control Tower, depois que você os habilita em qualquer OU específica.

- [SH.Athena.1] Os grupos de trabalho do Athena devem ser criptografados em repouso
- [SH.Neptune.1] Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [SH.Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- [SH.Neptune.3] Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [SH.Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [SH.Neptune.5] Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- [SH.Neptune.6] Os instantâneos do cluster de banco de dados Neptune devem ser criptografados em repouso
- [SH.Neptune.7] Os clusters de banco de dados Neptune devem ter IAM a autenticação de banco de dados ativada
- [SH.Neptune.8] Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [SH.RDS.27] Os clusters de RDS banco de dados devem ser criptografados em repouso

O novo AWS Security Hub controles de detetive estão disponíveis na maioria Regiões da AWS onde a AWS Control Tower está disponível. Para obter mais detalhes sobre esses controles, consulte Controles que se aplicam ao Service-Managed Standard: AWS Control Tower. Para obter mais detalhes sobre onde os controles estão disponíveis, consulteLimitações de controle.

## Novo tipo de desvio relatado: acesso confiável desativado

21 de setembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Depois de configurar sua zona de pouso da AWS Control Tower, você pode desativar o acesso confiável à AWS Control Tower em AWS Organizations. No entanto, isso causa desvio.

Com o tipo de desvio desativado com acesso confiável, a AWS Control Tower notifica você quando esse tipo de desvio ocorre, para que você possa reparar sua zona de pouso da AWS Control Tower. Para obter mais informações, consulte Tipos de deriva de governança.

## Quatro adicionais Regiões da AWS

13 de setembro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora está disponível na Ásia-Pacífico (Hyderabad), Europa (Espanha e Zurique) e Oriente Médio (). UAE

Se você já estiver usando o AWS Control Tower e quiser estender seus recursos de governança para essa região em suas contas, acesse a página Configurações no painel da AWS Control Tower, selecione a Região e atualize sua landing zone. Depois de atualizar a landing zone, você deve atualizar todas as contas que são administradas pela AWS Control Tower para colocar suas contas OUs sob controle na nova região. Para obter mais informações, consulte Sobre atualizações.

Para obter uma lista completa das regiões nas quais o AWS Control Tower está disponível, consulte o Região da AWS Tabela.

## AWSControl Tower disponível na região de Tel Aviv

28 de agosto de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower anuncia a disponibilidade na região de Israel (Tel Aviv).

Se você já estiver usando o AWS Control Tower e quiser estender seus recursos de governança para essa região em suas contas, acesse a página Configurações no painel da AWS Control Tower, selecione a Região e atualize sua landing zone. Depois de atualizar a landing zone, você deve atualizar todas as contas que são administradas pela AWS Control Tower para colocar suas contas OUs sob controle na nova região. Para obter mais informações, consulte Sobre atualizações.

Para obter uma lista completa das regiões nas quais o AWS Control Tower está disponível, consulte o Região da AWS Tabela.

## AWSControl Tower lança 28 novos controles proativos

24 de julho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower está adicionando 28 novos controles proativos, para ajudá-lo a gerenciar seu AWS meio ambiente.

Os controles proativos aprimoram os recursos de governança do AWS Control Tower em suas várias contas AWS ambientes, bloqueando recursos não compatíveis antes de serem provisionados. Esses controles ajudam a gerenciar AWS serviços como Amazon CloudWatch, Amazon Neptune, Amazon, ElastiCache AWS Step Functions e Amazon DocumentDB. Os novos controles ajudam você a atingir objetivos de controle, como estabelecer registros e monitoramento, criptografar dados em repouso ou melhorar a resiliência.

Aqui está uma lista completa dos novos controles:

- [CT. APPSYNC.PR.1] Exigir um AWS AppSync O GraphQL API deve ter o registro ativado
- [CT. CLOUDWATCH.PR.1] Exija que um CloudWatch alarme da Amazon tenha uma ação configurada para o estado do alarme
- [CT. CLOUDWATCH.PR.2] Exija que um grupo de CloudWatch registros da Amazon seja mantido por pelo menos um ano
- [CT. CLOUDWATCH.PR.3] Exija que um grupo de CloudWatch log da Amazon seja criptografado em repouso com um AWS KMSchave
- [CT. CLOUDWATCH.PR.4] Exigir que uma ação de CloudWatch alarme da Amazon seja ativada
- [CT. DOCUMENTDB.PR.1] Exija que um cluster Amazon DocumentDB seja criptografado em repouso

- [CT. DOCUMENTDB.PR.2] Exija que um cluster Amazon DocumentDB tenha os backups automáticos habilitados
- [CT. DYNAMODB.PR.2] Exija que uma tabela do Amazon DynamoDB seja criptografada em repouso usando AWS KMS keys
- [CT. EC2.PR.13] Exija que uma EC2 instância da Amazon tenha o monitoramento detalhado ativado
- [CT. EKS.PR.1] Exija que um EKS cluster da Amazon seja configurado com o acesso público desativado ao endpoint do servidor Kubernetes do cluster API
- [CT. ELASTICACHE.PR.1] Exija que um cluster Amazon ElastiCache for Redis tenha os backups automáticos ativados
- [CT. ELASTICACHE.PR.2] Exija que um cluster Amazon ElastiCache for Redis tenha as atualizações automáticas de versões secundárias ativadas
- [CT. ELASTICACHE.PR.3] Exija que um grupo de replicação Amazon ElastiCache for Redis tenha o failover automático ativado
- [CT. ELASTICACHE.PR.4] Exigir que um grupo de ElastiCache replicação da Amazon tenha a criptografia em repouso ativada
- [CT. ELASTICACHE.PR.5] Exija que um grupo de replicação Amazon ElastiCache for Redis tenha a criptografia em trânsito ativada
- [CT. ELASTICACHE.PR.6] Exigir um cluster de ElastiCache cache da Amazon para usar um grupo de sub-rede personalizado
- [CT. ELASTICACHE.PR.7] Exija que um grupo de ElastiCache replicação da Amazon de versões anteriores do Redis tenha autenticação do Redis AUTH
- [CT. ELASTICBEANSTALK.PR.3] Exigir um AWS Ambiente Elastic Beanstalk para ter uma configuração de registro
- [CT. LAMBDA.PR.3] Exigir um AWS Lambda função para estar em uma Amazon Virtual Private Cloud () gerenciada pelo cliente VPC
- [CT. NEPTUNE.PR.1] Exija que um cluster de banco de dados Amazon Neptune tenha AWS Identity and Access Management (IAM) autenticação de banco de dados
- [CT. NEPTUNE.PR.2] Exija que um cluster de banco de dados Amazon Neptune tenha a proteção de exclusão ativada
- [CT. NEPTUNE.PR.3] Exija que um cluster de banco de dados Amazon Neptune tenha a criptografia de armazenamento ativada
- [CT. REDSHIFT.PR.8] Exigir que um cluster do Amazon Redshift seja criptografado

- [CT.S3.PR.9] Exija que um bucket do Amazon S3 tenha o S3 Object Lock ativado
- [CT.S3.PR.10] Exija que um bucket Amazon S3 tenha a criptografia do lado do servidor configurada usando AWS KMS keys
- [CT.S3.PR.11] Exija que um bucket do Amazon S3 tenha o versionamento ativado
- [CT. STEPFUNCTIONS.PR.1] Exigir um AWS Step Functions máquina de estado para ter o registro ativado
- [CT. STEPFUNCTIONS.PR.2] Exigir um AWS Step Functions máquina de estado para ter AWS X-Ray rastreamento ativado

Os controles proativos no AWS Control Tower são implementados por meio de AWS CloudFormation Ganchos, que identificam e bloqueiam recursos não compatíveis antes AWS CloudFormation os provisiona. Os controles proativos complementam os recursos de controle preventivo e de detetive existentes no AWS Control Tower.

Esses novos controles proativos estão disponíveis em todos Regiões da AWS onde a AWS Control Tower está disponível. Para obter mais detalhes sobre esses controles, consulte Controles proativos.

## AWSA Control Tower suspende o uso de dois controles

18 de julho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower realiza revisões regulares de seus controles de segurança para garantir que eles estejam atualizados e ainda sejam considerados as melhores práticas. Os dois controles a seguir foram descontinuados, a partir de 18 de julho de 2023, e serão removidos da biblioteca de controles a partir de 18 de agosto de 2023. Você não pode mais ativar esses controles em nenhuma unidade organizacional. Você pode optar por desativar esses controles antes da data de remoção.

- [SH.S3.4] Os buckets S3 devem ter a criptografia do lado do servidor ativada
- [CT.S3.PR.7] Exigir que um bucket Amazon S3 tenha a criptografia do lado do servidor configurada

Motivo da depreciação

Em janeiro de 2023, o Amazon S3 configurou a criptografia padrão em todos os buckets não criptografados novos e existentes para aplicar a criptografia do lado do servidor com chaves

gerenciadas do S3 SSE (-S3) como o nível básico de criptografia para novos objetos carregados nesses buckets. Nenhuma alteração foi feita na configuração de criptografia padrão de um bucket existente que já tinha SSE -S3 ou criptografia do lado do servidor com AWS Serviço de gerenciamento de chaves (AWS KMS) teclas (SSE-KMS) configuradas.

## AWSVersão 3.2 da zona de pouso da Control Tower

16 de junho de 2023

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 3.2. Para obter informações, consulteAtualize sua landing zone).

AWSA versão 3.2 da zona de pouso do Control Tower traz os controles que fazem parte do AWS Security Hub Padrão gerenciado por serviços: AWS Control Tower até disponibilidade geral. Ele introduz a capacidade de visualizar o status de deriva dos controles que fazem parte desse padrão no console AWS Control Tower.

Essa atualização inclui uma nova função vinculada ao serviço (SLR), chamada de. AWSServiceRoleForAWSControlTower Essa função auxilia a AWS Control Tower criando uma regra EventBridge gerenciada, chamada de AWSControlTowerManagedRuleem cada conta de membro. Essa regra gerenciada coleta AWS Security Hub Encontrar eventos com o AWS Control Tower pode determinar o desvio do controle.

Essa regra é a primeira regra gerenciada a ser criada pela AWS Control Tower. A regra não é implantada por uma pilha; ela é implantada diretamente do. EventBridge APIs Você pode ver a regra no EventBridge console ou por meio do EventBridge APIs. Se o `managed-by` campo for preenchido, ele mostrará o diretor de serviço da AWS Control Tower.

Anteriormente, a AWS Control Tower assumia a AWSControlTowerExecutionfunção de realizar operações nas contas dos membros. Essa nova função e regra estão melhor alinhadas com o princípio de melhores práticas de permitir o mínimo de privilégios ao realizar operações em uma conta múltipla AWS meio ambiente. A nova função fornece permissões reduzidas que permitem especificamente: criar a regra gerenciada nas contas dos membros, manter a regra gerenciada, publicar notificações de segurança e verificar o SNS desvio. Para obter mais informações, consulte AWSServiceRoleForAWSControlTower.

A atualização do landing zone 3.2 também inclui um novo StackSet recurso na conta de gerenciamentoBP_BASELINE_SERVICE_LINKED_ROLE, que inicialmente implanta a função vinculada ao serviço.

Ao relatar o desvio de controle do Security Hub (na landing zone 3.2 e versões posteriores), a AWS Control Tower recebe uma atualização de status diária do Security Hub. Embora os controles estejam ativos em todas as regiões governadas, a AWS Control Tower envia o AWS Security Hub Encontrar eventos somente na região de origem da AWS Control Tower. Para obter mais informações, consulte Relatórios de desvio de controle do Security Hub.

Atualização do controle Region Deny

Esta versão do landing zone também inclui uma atualização para o controle Region Deny.

Serviços globais e APIs adicionados

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) para permitir a visibilidade de eventos globais nas contas dos membros.
- AWS Faturamento consolidado () `consolidatedbilling:*`
- AWS Management Console Mobile Application (`consoleapp:*`)
- AWS Nível gratuito (`freetier:*`)
- Faturamento da AWS (`invoicing:*`)
- AWS QI () `iq:*`
- AWS Notificações do usuário (`notifications:*`)
- AWS Contatos de notificações do usuário (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS Configurações fiscais (`tax:*`)

Serviços globais e APIs removidos

- Removido `s3:GetAccountPublic` porque não é uma ação válida.
- Removido `s3:PutAccountPublic` porque não é uma ação válida.

## AWSA Control Tower gerencia contas com base em ID

14 de junho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora cria e gerencia contas que você cria no Account Factory rastreando o AWS ID da conta, em vez do endereço de e-mail da conta.

Ao provisionar uma conta, o solicitante da conta sempre deve ter as permissões `CreateAccount` e as. `DescribeCreateAccountStatus` Esse conjunto de permissões faz parte da função de administrador e é concedido automaticamente quando um solicitante assume a função de administrador. Se você delegar permissão para provisionar contas, talvez seja necessário adicionar essas permissões diretamente para os solicitantes da conta.

## Controles de detetive adicionais do Security Hub disponíveis na biblioteca de controles da AWS Control Tower

12 de junho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower adicionou dez novos AWS Security Hub controles de detetive para a biblioteca de controles da AWS Control Tower. Esses novos controles têm como alvo serviços como API Gateway, AWS CodeBuild, Amazon Elastic Compute Cloud (EC2), Amazon Elastic Load Balancer, Amazon Redshift, Amazon e SageMaker AWS WAF. Esses novos controles ajudam você a aprimorar sua postura de governança atendendo aos objetivos de controle, como estabelecer registros e monitoramento, limitar o acesso à rede e criptografar dados em repouso.

Esses controles agem como parte do Security Hub Service-Managed Standard: AWS Control Tower, depois que você os habilita em qualquer OU específica.

- [sh.Account.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS
- [ELA. APIGateway.8] As rotas de API gateway devem especificar um tipo de autorização
- [ELA. APIGateway.9] O registro de acesso deve ser configurado para os estágios do API Gateway V2
- [ELA. CodeBuild.3] Os registros CodeBuild do S3 devem ser criptografados
- [ELA. EC2.25] os modelos de EC2 lançamento não devem atribuir interfaces públicas IPs às de rede
- [ELA. ELB.1] O Application Load Balancer deve ser configurado para HTTP redirecionar todas as solicitações para HTTPS
- [sh.Redshift.10] Os clusters do Redshift devem ser criptografados em repouso

- [ELA. SageMaker.2] As instâncias do SageMaker notebook devem ser iniciadas de forma personalizada VPC
- [ELA. SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [ELA. WAF.10] Uma WAFV2 web ACL deve ter pelo menos uma regra ou grupo de regras

O novo AWS Security Hub controles de detetive estão disponíveis em todos Regiões da AWS onde a AWS Control Tower está disponível. Para obter mais detalhes sobre esses controles, consulte Controles que se aplicam ao Service-Managed Standard: AWS Control Tower.

## AWSA Control Tower publica tabelas de metadados de controle

7 de junho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora fornece tabelas completas de metadados de controle como parte da documentação publicada. Ao trabalhar com o controleAPIs, você pode consultar cada controle APIcontrolIdentifier, que é exclusivo ARN associado a cada um Região da AWS. As tabelas incluem as estruturas e os objetivos de controle que cada controle abrange. Anteriormente, essas informações estavam disponíveis somente no console.

As tabelas também incluem os metadados dos controles do Security Hub que fazem parte do AWS Security Hub Padrão gerenciado por serviços: AWS Control Tower. Para obter detalhes completos, consulte Tabelas de metadados de controle.

Para obter uma lista abreviada de identificadores de controle e alguns exemplos de uso, consulte Identificadores de recursos e controles. APIs

## Suporte do Terraform para Account Factory Customization

6 de junho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower oferece suporte em uma única região para o Terraform por meio da Customização de Fábrica de Conta (). AFC A partir desta versão, você pode usar o AWS Control Tower e o Service Catalog juntos para definir esquemas de AFC contas no Terraform open source. Você pode personalizar seu novo e o existente Contas da AWS, antes de provisionar recursos na

AWS Control Tower. Por padrão, esse recurso permite que você implante e atualize contas, com o Terraform, na sua região de origem da AWS Control Tower.

Um esquema de conta descreve os recursos e configurações específicos que são necessários quando um Conta da AWS é provisionado. Você pode usar o blueprint como modelo para criar vários Contas da AWS em grande escala.

Para começar, use o Terraform Reference Engine ativado. GitHub O Reference Engine configura o código e a infraestrutura necessários para que o mecanismo de código aberto Terraform funcione com o Service Catalog. Esse processo de configuração único leva alguns minutos. Depois disso, você pode definir seus requisitos de conta personalizados no Terraform e, em seguida, implantar suas contas com o fluxo de trabalho bem definido da fábrica de contas da AWS Control Tower. Os clientes que preferem trabalhar com o Terraform podem utilizar a personalização de contas do AWS Control Tower em grande escala e obter acesso imediato a cada conta após o provisionamento. AFC

Para saber como criar essas personalizações, consulte Creating Products and Getting started with Terraform open source na documentação do Service Catalog. Esse recurso está disponível em todos Regiões da AWS onde a AWS Control Tower está disponível.

## AWS IAMAutogerenciamento do Identity Center disponível para landing zone

6 de junho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora oferece suporte a uma opção opcional de provedor de identidade para uma landing zone da AWS Control Tower, que você pode configurar durante a instalação ou atualização. Por padrão, a landing zone está autorizada a usar AWS IAMIdentity Center, em alinhamento com as diretrizes de melhores práticas definidas em Organizing Your AWS Ambiente usando várias contas. Agora você tem três alternativas:

- Você pode aceitar o padrão e permitir que a AWS Control Tower configure e gerencie AWS IAMIdentity Center para você.
- Você pode optar por se autogerenciar AWS IAMIdentity Center, para refletir seus requisitos comerciais específicos.
- Opcionalmente, você pode trazer e autogerenciar um provedor de identidade terceirizado, conectando-o por meio do IAM Identity Center, se necessário. Você deve usar a opcionalidade de

provedor de identidade se seu ambiente regulatório exigir o uso de um provedor específico ou se você operar em Regiões da AWS where AWS IAMO Identity Center não está disponível.

Para obter mais informações, consulte IAMOrientação do Identity Center.

A seleção de provedores de identidade no nível da conta não é suportada. Esse recurso se aplica somente à landing zone como um todo. AWSA opcionalidade do provedor de identidade Control Tower está disponível em todos Regiões da AWS onde a AWS Control Tower está disponível.

## AWSControl Tower aborda a governança mista para OUs

1 de junho de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Com essa versão, o AWS Control Tower impede a implantação de controles em uma unidade organizacional (OU), se essa OU estiver em um estado de governança mista. A governança mista ocorre em uma OU se as contas não forem atualizadas após a AWS Control Tower estender a governança para uma nova Região da AWS, ou remove a governança. Esta versão ajuda você a manter as contas dos membros dessa OU em conformidade uniforme. Para obter mais informações, consulte Evite governança mista ao configurar regiões.

## Controles proativos adicionais disponíveis

19 de maio de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower está adicionando 28 novos controles proativos para ajudá-lo a governar seu ambiente de várias contas e atingir objetivos de controle específicos, como criptografia de dados em repouso ou limitar o acesso à rede. Os controles proativos são implementados com AWS CloudFormation ganchos que verificam seus recursos antes de serem provisionados. Os novos controles podem ajudar a governar AWS serviços como Amazon OpenSearch Service, Amazon EC2 Auto Scaling, Amazon, Amazon API Gateway e SageMaker Amazon Relational Database Service (). RDS

Controles proativos são suportados em todas as áreas comerciais Regiões da AWS onde a AWS Control Tower está disponível.

OpenSearch Serviço Amazon

- [CT. OPENSEARCH.PR.1] Exigir um domínio do Elasticsearch para criptografar dados em repouso
- [CT. OPENSEARCH.PR.2] Exigir que um domínio Elasticsearch seja criado em uma Amazon especificada pelo usuário VPC
- [CT. OPENSEARCH.PR.3] Exigir um domínio do Elasticsearch para criptografar dados enviados entre os nós
- [CT. OPENSEARCH.PR.4] Exigir um domínio do Elasticsearch para enviar registros de erros para o Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.5] Exigir um domínio do Elasticsearch para enviar registros de auditoria para o Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.6] Exija que um domínio do Elasticsearch tenha reconhecimento de zona e pelo menos três nós de dados
- [CT. OPENSEARCH.PR.7] Exija que um domínio do Elasticsearch tenha pelo menos três nós principais dedicados
- [CT. OPENSEARCH.PR.8] Exigir um domínio do Elasticsearch Service para usar .2 TLSv1
- [CT. OPENSEARCH.PR.9] Exigir um domínio do Amazon OpenSearch Service para criptografar dados em repouso
- [CT. OPENSEARCH.PR.10] Exigir que um domínio do Amazon OpenSearch Service seja criado em uma Amazon especificada pelo usuário VPC
- [CT. OPENSEARCH.PR.11] Exigir um domínio do Amazon OpenSearch Service para criptografar dados enviados entre os nós
- [CT. OPENSEARCH.PR.12] Exigir um domínio do Amazon OpenSearch Service para enviar registros de erros para o Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.13] Exigir um domínio do Amazon OpenSearch Service para enviar registros de auditoria para o Amazon Logs CloudWatch
- [CT. OPENSEARCH.PR.14] Exija que um domínio do Amazon OpenSearch Service tenha reconhecimento de zona e pelo menos três nós de dados
- [CT. OPENSEARCH.PR.15] Exija um domínio do Amazon OpenSearch Service para usar um controle de acesso refinado
- [CT. OPENSEARCH.PR.16] Exigir um domínio do Amazon OpenSearch Service para usar .2 TLSv1

### Amazon EC2 Auto Scaling

- [CT. AUTOSCALING.PR.1] Exija que um grupo do Amazon EC2 Auto Scaling tenha várias zonas de disponibilidade
- [CT. AUTOSCALING.PR.2] Exija uma configuração de lançamento de grupo do Amazon EC2 Auto Scaling para configurar instâncias da Amazon para EC2 IMDSv2
- [CT. AUTOSCALING.PR.3] Exija que uma configuração de lançamento do Amazon EC2 Auto Scaling tenha um limite de resposta de metadados de salto único
- [CT. AUTOSCALING.PR.4] Exija que um grupo do Amazon EC2 Auto Scaling associado a um Amazon Elastic Load Balancing () tenha as verificações de saúde ativadas ELB ELB
- [CT. AUTOSCALING.PR.5] Exija que uma configuração de lançamento de grupo do Amazon EC2 Auto Scaling não tenha instâncias da Amazon EC2 com endereços IP públicos
- [CT. AUTOSCALING.PR.6] Exija que qualquer grupo do Amazon EC2 Auto Scaling use vários tipos de instância
- [CT. AUTOSCALING.PR.8] Exija que um grupo do Amazon EC2 Auto Scaling tenha modelos de lançamento configurados EC2

### Amazon SageMaker

- [CT. SAGEMAKER.PR.1] Exigir uma instância de SageMaker notebook da Amazon para impedir o acesso direto à Internet
- [CT. SAGEMAKER.PR.2] Exija que as instâncias de SageMaker notebook da Amazon sejam implantadas em uma Amazon personalizada VPC
- [CT. SAGEMAKER.PR.3] Exija que as instâncias de SageMaker notebook da Amazon tenham acesso root não permitido

### Amazon API Gateway

- [CT. APIGATEWAY.PR.5] Exija que o Amazon API Gateway V2 Websocket e HTTP as rotas especifiquem um tipo de autorização

### Amazon Relational Database Service RDS ()

- [CT. RDS.PR.25] Exigir que um cluster de RDS banco de dados da Amazon tenha o registro configurado

Para obter mais informações, consulte Controles proativos.

## Controles EC2 proativos atualizados da Amazon

2 de maio de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSA Control Tower atualizou dois controles proativos: CT.EC2.PR.3 e CT.EC2.PR.4.

Para o atualizado CT.EC2.PR.3 controle, qualquer AWS CloudFormation A implantação que faz referência a uma lista de prefixos para um recurso do grupo de segurança está bloqueada, a menos que seja para a porta 80 ou 443.

Para o atualizado CT.EC2.PR.4 controle, qualquer AWS CloudFormation A implantação que faz referência a uma lista de prefixos para um recurso de grupo de segurança é bloqueada se a porta for 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 21, 1434, 4333, 5432, 5500, 5601, 22, 3000, 5000, 8088, 8888.

## Sete adicionais Regiões da AWS available

19 de abril de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora está disponível em mais sete Regiões da AWS: Norte da Califórnia (São Francisco), Ásia-Pacífico (Hong Kong, Jacarta e Osaka), Europa (Milão), Oriente Médio (Bahrein) e África (Cidade do Cabo). Essas regiões adicionais do AWS Control Tower, chamadas de regiões opcionais, não estão ativas por padrão, exceto a região Oeste dos EUA (Norte da Califórnia), que está ativa por padrão.

Alguns controles no AWS Control Tower não operam em alguns desses controles adicionais Regiões da AWS onde a AWS Control Tower está disponível, porque essas regiões não oferecem suporte à funcionalidade subjacente necessária. Para obter detalhes, consulte Limitações de controle.

Entre essas novas regiões, o cFCT não está disponível na Ásia-Pacífico (Jacarta e Osaka). Disponibilidade em outros Regiões da AWS está inalterado.

Para obter mais informações sobre como a AWS Control Tower gerencia as limitações de regiões e controles, consulteConsiderações sobre a ativação de regiões opcionais AWS.

Os VPCe endpoints exigidos pelo não AFT estão disponíveis na região Oriente Médio (Bahrein). Os clientes que estão implantando AFT nesta região devem implantar com parâmetros`aft_vpc_endpoints=false`. Para obter mais informações, consulte o parâmetro no README arquivo.

AWSA Control Tower VPCs tem duas zonas de disponibilidade na região Oeste dos EUA (Norte da Califórnia)`us-west-1`, devido a uma limitação na AmazonEC2. No Oeste dos EUA (Norte da Califórnia), seis sub-redes são divididas em duas zonas de disponibilidade. Para obter mais informações, consulte Visão geral do AWS Control Tower e das VPCs.

AWSA Control Tower adicionou novas permissões `AWSControlTowerServiceRolePolicy` que permitem que a AWS Control Tower faça chamadas para o `EnableRegionListRegions`,, e `GetRegionOptStatus` APIs implementadas pelo AWS Serviço de gerenciamento de contas, para torná-los adicionais Regiões da AWS disponível para suas contas compartilhadas na landing zone (conta de gerenciamento, conta de arquivamento de registros, conta de auditoria) e suas contas de membros da OU. Para obter mais informações, consulte Políticas gerenciadas para o AWS Control Tower.

## Account Factory para rastreamento de solicitações de personalização de conta do Terraform (AFT)

16 de fevereiro de 2023

AFToferece suporte ao rastreamento de solicitações de personalização da conta. Toda vez que você envia uma solicitação de personalização da conta, AFT gera um token de rastreamento exclusivo que passa por uma personalização AFT AWS Step Functions máquina de estado, que registra o token como parte de sua execução. Você pode usar as consultas de insights do Amazon CloudWatch Logs para pesquisar intervalos de timestamp e recuperar o token da solicitação. Como resultado, você pode ver as cargas que acompanham o token, para que você possa rastrear sua solicitação de personalização da conta em todo AFT o fluxo de trabalho. Para obter mais informações sobreAFT, consulte Visão geral do AWS Control Tower Account Factory for Terraform. Para obter informações sobre CloudWatch Logs e Step Functions, consulte o seguinte:

- O que é Amazon CloudWatch Logs? no Guia do usuário do Amazon CloudWatch Logs
- O que é AWS Step Functions? no AWS Step Functions Guia do desenvolvedor

# AWSVersão 3.1 da zona de pouso da Control Tower

9 de fevereiro de 2023

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 3.1. Para obter informações, consulteAtualize sua landing zone)

AWSA versão 3.1 da zona de pouso do Control Tower inclui as seguintes atualizações:

- Com esta versão, o AWS Control Tower desativa o registro de acesso desnecessário para seu bucket de registro de acesso, que é o bucket do Amazon S3 em que os registros de acesso são armazenados na conta do Log Archive, enquanto continua habilitando o registro de acesso ao servidor para buckets do S3. Esta versão também inclui atualizações no controle Region Deny que permitem ações adicionais para serviços globais, como AWS Support Planos e AWS Artifact.
- A desativação do registro de acesso ao servidor para o bucket de registro de acesso da AWS Control Tower faz com que o Security Hub crie uma descoberta para o intervalo de registro de acesso da conta Log Archive, devido a um AWS Security Hub regra, [S3.9] O registro de acesso ao servidor bucket S3 deve estar habilitado. Em alinhamento com o Security Hub, recomendamos que você suprima essa descoberta específica, conforme declarado na descrição dessa regra no Security Hub. Para obter informações adicionais, consulte informações sobre descobertas suprimidas.
- O registro de acesso para o bucket de registro (regular) na conta do Log Archive permanece inalterado na versão 3.1. De acordo com as melhores práticas, os eventos de acesso desse intervalo são registrados como entradas de registro no intervalo de registro de acesso. Para obter mais informações sobre o registro de acesso, consulte Registro de solicitações usando o registro de acesso ao servidor na documentação do Amazon S3.
- Fizemos uma atualização do controle Region Deny. Essa atualização permite ações de mais serviços globais. Para obter detalhes sobre issoSCP, consulte Negar acesso a AWS com base no solicitado Região da AWSe controles que aprimoram a proteção da residência de dados.

  Serviços globais adicionados:

  - AWS Account Management (`account:*`)
  - AWS Ativar (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)
  - AWS Compute Optimizer (`compute-optimizer:*`)

- AWS Data Pipeline (`datapipeline:GetAccountLimits`)
- AWS Device Farm(`devicefarm:*`)
- AWS Marketplace (`discovery-marketplace:*`)
- Amazon ECR (`ecr-public:*`)
- AWS License Manager (`license-manager:ListReceivedLicenses`)
- AWS `lightsail:Get*`Lightsail ()
- Explorador de recursos da AWS (`resource-explorer-2:*`)
- Amazon S3 (`s3:CreateMultiRegionAccessPoint`,,`s3:GetBucketPolicyStatus`) `s3:PutMultiRegionAccessPointPolicy`
- AWS Savings Plans (`savingsplans:*`)
- IAMCentro de identidade (`sso:*`)
- AWS Support App (`supportapp:*`)
- AWS Support Planos (`supportplans:*`)
- AWS Sustentabilidade (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Informações do fornecedor () `vendor-insights:ListEntitledSecurityProfiles`

### Controles proativos geralmente disponíveis

24 de janeiro de 2023

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

Os controles proativos opcionais, anunciados anteriormente no status de pré-visualização, agora estão disponíveis ao público em geral. Esses controles são chamados de proativos porque verificam seus recursos — antes de serem implantados — para determinar se os novos recursos estão em conformidade com os controles ativados em seu ambiente. Para obter mais informações, consulte Controles abrangentes auxiliam na AWS provisionamento e gerenciamento de recursos.

## Janeiro a dezembro de 2022

Em 2022, a AWS Control Tower lançou as seguintes atualizações:

- Operações de conta simultânea

- Personalização da Account Factory () AFC
- Controles abrangentes auxiliam na AWS provisionamento e gerenciamento de recursos
- Status de conformidade visível para todos AWS Config regras
- APIpara controles e um novo AWS CloudFormation recurso
- O cFct suporta a exclusão do conjunto de pilhas
- Retenção de registros personalizada
- Reparo de desvio de função disponível
- AWSVersão 3.0 da zona de pouso da Control Tower
- A página Organização combina visualizações OUs e contas
- Inscrição e atualização mais fáceis para contas de membros individuais
- AFTsuporta personalização automatizada para contas compartilhadas da AWS Control Tower
- Operações simultâneas para todos os controles opcionais
- Contas de segurança e registro existentes
- AWSVersão 2.9 da zona de pouso da Control Tower
- AWSVersão 2.8 da zona de pouso da Control Tower

## Operações de conta simultânea

16 de dezembro de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora suporta ações simultâneas na fábrica de contas. Você pode criar, atualizar ou inscrever até cinco (5) contas por vez. Envie até cinco ações consecutivas e veja o status de conclusão de cada solicitação, enquanto suas contas terminam de ser criadas em segundo plano. Por exemplo, você não precisa mais esperar que cada processo seja concluído antes de atualizar outra conta ou antes de registrar novamente uma unidade organizacional (OU) inteira.

## Personalização da Account Factory () AFC

28 de novembro de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

A personalização de fábrica de contas permite que você personalize contas novas e existentes no console do AWS Control Tower. Esses novos recursos de personalização oferecem a flexibilidade

de definir planos de conta, que são AWS CloudFormation modelos contidos em um produto especializado do Service Catalog. Os blueprints fornecem recursos e configurações totalmente personalizados. Você também pode escolher usar plantas predefinidas, criadas e gerenciadas por AWS parceiros, que ajudam você a personalizar contas para casos de uso específicos.

Anteriormente, a fábrica de contas da AWS Control Tower não suportava a personalização de contas no console. Com essa atualização do Account Factory, você pode predefinir os requisitos da conta e implementá-los como parte de um fluxo de trabalho bem definido. Você pode aplicar esquemas para criar novas contas, para inscrever outras AWS contas na AWS Control Tower e para atualizar as contas existentes da AWS Control Tower.

Ao provisionar, inscrever ou atualizar uma conta na fábrica de contas, você selecionará o blueprint a ser implantado. Esses recursos especificados no blueprint são provisionados em sua conta. Quando sua conta terminar de ser criada, todas as configurações personalizadas estarão disponíveis para uso imediato.

Para começar a personalizar contas, você pode definir os recursos para o caso de uso pretendido em um produto do Service Catalog. Você também pode selecionar soluções gerenciadas por parceiros no AWS Biblioteca de introdução. Para obter mais informações, consulte Personalize contas com Account Factory Customization (AFC).

## Controles abrangentes auxiliam na AWS provisionamento e gerenciamento de recursos

28 de novembro de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora oferece suporte ao gerenciamento abrangente de controles, incluindo novos controles proativos opcionais, implementados por meio de AWS CloudFormation ganchos. Esses controles são chamados de proativos porque verificam seus recursos — antes de serem implantados — para determinar se os novos recursos estarão em conformidade com os controles ativados em seu ambiente.

Mais de 130 novos controles proativos ajudam você a atingir objetivos políticos específicos para seu ambiente de AWS Control Tower; a atender aos requisitos das estruturas de conformidade padrão do setor; e a governar as interações da Control Tower AWS em mais de vinte outros AWS serviços.

A biblioteca de controles da AWS Control Tower classifica esses controles de acordo com os associados AWS serviços e recursos. Para obter mais detalhes, consulte Controles proativos.

Com esta versão, o AWS Control Tower também está integrado com AWS Security Hub, por meio do novo padrão gerenciado por serviços do Security Hub: AWS Control Tower, que suporta o AWS Padrão básico de melhores práticas de segurança (FSBP). Você pode ver mais de 160 controles do Security Hub junto com os controles da AWS Control Tower no console e obter uma pontuação de segurança do Security Hub para seu ambiente da AWS Control Tower. Para obter mais informações, consulte Controles do Security Hub.

## Status de conformidade visível para todos AWS Config regras

18 de novembro de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora exibe o status de conformidade de todos AWS Config regras implantadas em unidades organizacionais registradas na AWS Control Tower. Você pode ver o status de conformidade de todos AWS Config regras que afetam suas contas na AWS Control Tower, inscritas ou não inscritas, sem sair do console da Control TowerAWS. Os clientes podem optar por configurar as regras do Config, chamadas de controles de detetive, na AWS Control Tower ou configurá-las diretamente por meio do AWS Config serviço. As regras implantadas pelo AWS Config são mostradas, junto com as regras implantadas pela AWS Control Tower.

Anteriormente, AWS Config regras implantadas por meio do AWS Config o serviço não estava visível no console do AWS Control Tower. Os clientes precisavam navegar até o AWS Config serviço para identificar não conformidades AWS Config regras. Agora você pode identificar qualquer não compatível AWS Config regra dentro do console AWS Control Tower. Para ver o status de conformidade de todas as suas regras do Config, navegue até a página de detalhes da conta no console do AWS Control Tower. Você verá uma lista mostrando o status de conformidade dos controles gerenciados pelas regras AWS Control Tower e Config implantadas fora da Control TowerAWS.

## APIpara controles e um novo AWS CloudFormation recurso

1º de setembro de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora suporta o gerenciamento programático de controles, também conhecido como grades de proteção, por meio de um conjunto de chamadas. API Um novo AWS CloudFormation O recurso suporta a API funcionalidade dos controles. Para obter mais detalhes,

consulte Automatize tarefas no AWS Control Tower e Crie AWS Control Tower recursos com AWS CloudFormation.

Eles APIs permitem que você ative, desative e visualize o status do aplicativo dos controles na biblioteca AWS Control Tower. Eles APIs incluem suporte para AWS CloudFormation, para que você possa gerenciar AWS recursos como infrastructure-as-code (IAc). AWSO Control Tower fornece controles preventivos e de deteção opcionais que expressam suas intenções políticas em relação a toda uma unidade organizacional (OU) e a cada AWS conta dentro da OU. Essas regras permanecem em vigor à medida que você cria novas contas ou faz alterações nas contas existentes.

APIsincluído nesta versão

- EnableControl— Essa API chamada ativa um controle. Ele inicia uma operação assíncrona que cria AWS recursos na unidade organizacional especificada e nas contas que ela contém.
- DisableControl— Essa API chamada desliga um controle. Ele inicia uma operação assíncrona que exclui AWS recursos na unidade organizacional especificada e nas contas que ela contém.
- GetControlOperation— Retorna o status de uma determinada DisableControloperação EnableControlou operação.
- ListEnabledControls— Lista os controles ativados pelo AWS Control Tower na unidade organizacional especificada e nas contas que ela contém.

Para ver uma lista de nomes de controle para controles opcionais, consulte Identificadores de recursos APIs e controles, no AWSControl Tower User Guide.

## O cFct suporta a exclusão do conjunto de pilhas

26 de agosto de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

As personalizações do AWS Control Tower (cFct) agora oferecem suporte à exclusão de conjuntos de pilhas, definindo um parâmetro no arquivo. `manifest.yaml` Para obter mais informações, consulte Excluir um conjunto de pilhas.

> **Important**
>
> Quando você define inicialmente o valor de `enable_stack_set_deletion` para`true`, na próxima vez que invocar o cFct, ALLos recursos que começam com

o prefixo`CustomControlTower-`, que têm a tag `Key:AWS_Solutions, Value: CustomControlTowerStackSet` de chave associada e que não são declarados no arquivo de manifesto, são preparados para exclusão.

## Retenção de registros personalizada

15 de agosto de 2022

(Atualização necessária para a landing zone da AWS Control Tower. Para obter informações, consulteAtualize sua landing zone)

AWSO Control Tower agora oferece a capacidade de personalizar a política de retenção para buckets do Amazon S3 que armazenam seus registros da AWS Control Tower. CloudTrail Você pode personalizar sua política de retenção de logs do Amazon S3, em incrementos de dias ou anos, até um máximo de 15 anos.

Se você optar por não personalizar sua retenção de registros, as configurações padrão são 1 ano para registro de conta padrão e 10 anos para registro de acesso.

Esse recurso está disponível para clientes existentes por meio da AWS Control Tower quando você atualiza ou repara sua landing zone, e para novos clientes por meio do processo de configuração da AWS Control Tower.

## Reparo de desvio de função disponível

11 de agosto de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora suporta reparo em caso de desvio de função. Você pode restaurar uma função necessária sem um reparo completo da sua landing zone. Se esse tipo de reparo de deriva for necessário, a página de erro do console fornece etapas para restaurar a função, para que sua landing zone esteja novamente disponível.

## AWSVersão 3.0 da zona de pouso da Control Tower

29 de julho de 2022

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 3.0. Para obter informações, consulteAtualize sua landing zone)

AWSA versão 3.0 da zona de pouso do Control Tower inclui as seguintes atualizações:

- A opção de escolher o nível da organização AWS CloudTrail trilhas ou para optar por não participar das CloudTrail trilhas gerenciadas pela AWS Control Tower.
- Dois novos controles de detetive para determinar se AWS CloudTrail está registrando atividades em suas contas.
- A opção de agregar AWS Config informações sobre recursos globais somente em sua região de origem.
- Uma atualização para a Região nega o controle.
- Uma atualização da política gerenciada, AWSControlTowerServiceRolePolicy.
- Não criamos mais a IAM função `aws-controltower-CloudWatchLogsRole` e o grupo de CloudWatch registros `aws-controltower/CloudTrailLogs` em cada conta inscrita. Anteriormente, nós os criávamos em cada conta para sua trilha de conta. Com trilhas organizacionais, criamos apenas uma na conta de gerenciamento.

As seções a seguir fornecem mais detalhes sobre cada novo recurso.

CloudTrail Trilhas em nível organizacional na Control Tower AWS

Com a versão 3.0 do landing zone, o AWS Control Tower agora suporta o nível da organização AWS CloudTrail trilhas.

Ao atualizar sua zona de pouso do AWS Control Tower para a versão 3.0, você tem a opção de selecionar o nível da organização AWS CloudTrail trilhas conforme sua preferência de exploração madeireira, ou para optar por não participar das CloudTrail trilhas gerenciadas pela AWS Control Tower. Quando você atualiza para a versão 3.0, o AWS Control Tower exclui as trilhas existentes em nível de conta para contas inscritas após um período de espera de 24 horas. AWSO Control Tower não exclui trilhas em nível de conta para contas não inscritas. No caso improvável de a atualização da sua landing zone não ser bem-sucedida, mas a falha ocorrer após a AWS Control Tower já ter criado a trilha no nível da organização, você poderá incorrer em cobranças duplicadas pelas trilhas no nível da organização e da conta, até que sua operação de atualização seja concluída com êxito.

A partir da landing zone 3.0, a AWS Control Tower não suporta mais trilhas em nível de conta que AWS gerencia. Em vez disso, o AWS Control Tower cria uma trilha no nível da organização, que é ativa ou inativa, de acordo com sua seleção.

> **Note**
>
> Depois de atualizar para a versão 3.0 ou posterior, você não tem a opção de continuar com as CloudTrail trilhas no nível da conta gerenciadas pela AWS Control Tower.

Nenhum dado de registro é perdido dos seus registros de conta agregados, porque os registros permanecem no bucket existente do Amazon S3, onde estão armazenados. Somente as trilhas são excluídas, não os registros existentes. Se você selecionar a opção de adicionar trilhas em nível organizacional, o AWS Control Tower abrirá um novo caminho para uma nova pasta dentro do seu bucket do Amazon S3 e continuará enviando informações de registro para esse local. Se você optar por não participar das trilhas gerenciadas pela AWS Control Tower, seus registros existentes permanecerão no repositório, inalterados.

Convenções de nomenclatura de caminhos para armazenamento de registros

- Os registros de rastreamento da conta são armazenados com um caminho deste formato: `/org id/AWSLogs/…`
- Os registros de trilhas da organização são armazenados com um caminho deste formato: `/org id/AWSLogs/org id/…`

O caminho que o AWS Control Tower cria para suas CloudTrail trilhas no nível da organização é diferente do caminho padrão para uma trilha no nível da organização criada manualmente, que teria o seguinte formato:

- `/AWSLogs/org id/…`

Para obter mais informações sobre a nomenclatura de CloudTrail caminhos, consulte Encontrando seus arquivos de CloudTrail log.

> **Tip**
>
> Se você planeja criar e gerenciar suas próprias trilhas em nível de conta, recomendamos que você crie as novas trilhas antes de concluir a atualização para a versão 3.0 da zona de pouso do AWS Control Tower, para começar a registrar imediatamente.

A qualquer momento, você pode optar por criar novas CloudTrail trilhas no nível da conta ou da organização e gerenciá-las por conta própria. A opção de escolher CloudTrail trilhas em nível organizacional gerenciadas pelo AWS Control Tower está disponível durante qualquer atualização da landing zone para a versão 3.0 ou posterior. Você pode ativar e desativar trilhas em nível organizacional sempre que atualizar sua landing zone.

Se seus registros forem gerenciados por um serviço terceirizado, forneça o nome do novo caminho para seu serviço.

> **Note**
>
> Para zonas de pouso na versão 3.0 ou posterior, no nível da conta AWS CloudTrail trilhas não são suportadas pela AWS Control Tower. Você pode criar e manter suas próprias trilhas em nível de conta a qualquer momento, ou pode optar por trilhas em nível de organização gerenciadas pela Control Tower. AWS

Registro AWS Config recursos somente na região de origem

Na versão 3.0 do landing zone, a AWS Control Tower atualizou a configuração básica para AWS Config para que ele registre recursos globais somente na região de origem. Depois de atualizar para a versão 3.0, a gravação de recursos globais é ativada somente na sua região de origem.

Essa configuração é considerada uma prática recomendada. É recomendado por AWS Security Hub e AWS Config, e gera economia de custos ao reduzir o número de itens de configuração criados quando recursos globais são criados, modificados ou excluídos. Anteriormente, sempre que um recurso global era criado, atualizado ou excluído, seja por um cliente ou por um AWS serviço, um item de configuração foi criado para cada item em cada região governada.

Dois novos controles de detetive para AWS CloudTrail registro

Como parte da mudança para o nível organizacional AWS CloudTrail trails, a AWS Control Tower está introduzindo dois novos controles de detetive que verificam se CloudTrail está ativado. O primeiro controle tem orientação obrigatória e é ativado na OU de segurança durante as atualizações de configuração ou landing zone da 3.0 e versões posteriores. O segundo controle tem uma orientação altamente recomendada e é aplicado opcionalmente a qualquer OUs outro que não seja a UO de Segurança, que já tem a proteção de controle obrigatória aplicada.

Controle obrigatório: detecte se as contas compartilhadas na unidade organizacional de Segurança têm AWS CloudTrail ou CloudTrail Lake ativado

Controle altamente recomendado: detecte se uma conta tem AWS CloudTrail ou CloudTrail Lake ativado

Para obter mais informações sobre os novos controles, consulte a biblioteca de controles da AWS Control Tower.

Uma atualização para a Região nega o controle

Atualizamos a NotActionlista na Região de negação de controle para incluir ações de alguns serviços adicionais, listados abaixo:

```
“chatbot:*”,
"s3:GetAccountPublic",
"s3:DeleteMultiRegionAccessPoint",
"s3:DescribeMultiRegionAccessPointOperation",
"s3:GetMultiRegionAccessPoint",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetMultiRegionAccessPointPolicyStatus",
"s3:ListMultiRegionAccessPoints",
"s3:GetStorageLensConfiguration",
“s3:GetStorageLensDashboard",
“s3:ListStorageLensConfigurations”
“s3:GetAccountPublicAccessBlock“,,
“s3:PutAccountPublic",
“s3:PutAccountPublicAccessBlock“,
```

### Passo a passo em vídeo

Este vídeo (3:07) descreve como atualizar sua zona de pouso existente da AWS Control Tower para a versão 3. Para uma melhor visualização, selecione o ícone no canto inferior direito do vídeo para ampliá-lo em tela cheia. A legenda está disponível.

Passo a passo em vídeo da atualização de uma zona de pouso existente da AWS Control Tower para a zona de pouso 3.

## A página Organização combina visualizações OUs e contas

18 de julho de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

A nova página Organização no AWS Control Tower mostra uma visão hierárquica de todas as unidades organizacionais (OUs) e contas. Ele combina as informações das páginas OUse Contas, que existiam anteriormente.

Na nova página, você pode ver as relações entre os pais OUs e suas contas aninhadasOUs. Você pode agir em agrupamentos de recursos. Você pode configurar a visualização da página. Por exemplo, você pode expandir ou reduzir a exibição hierárquica, filtrar a exibição para ver contas ou OUs somente, optar por visualizar somente suas contas inscritas e registradasOUs, ou você pode visualizar grupos de recursos relacionados. É mais fácil garantir que toda a organização seja atualizada adequadamente.

## Inscrição e atualização mais fáceis para contas de membros individuais

31 de maio de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora oferece uma capacidade aprimorada de atualizar e inscrever contas de membros individualmente. Cada conta mostra quando está disponível para uma atualização, para que você possa garantir mais facilmente que suas contas de membros incluam a configuração mais recente. Você pode atualizar sua landing zone, corrigir o desvio da conta ou inscrever uma conta em uma OU registrada, em algumas etapas simplificadas.

Quando você atualiza uma conta, não é necessário incluir toda a unidade organizacional (OU) da conta em cada ação de atualização. Como resultado, o tempo necessário para atualizar uma conta individual é bastante reduzido.

Você pode inscrever contas na AWS Control Tower OUs com mais ajuda do console da AWS Control Tower. As contas existentes que você inscreve no AWS Control Tower ainda devem atender aos pré-requisitos da conta, e você deve adicionar a função. `AWSControlTowerExecution` Em seguida, você pode escolher qualquer OU registrada e inscrever a conta nela selecionando o botão Inscrever.

Separamos a funcionalidade Inscrever conta do fluxo de trabalho Criar conta na fábrica de contas para criar mais distinção entre esses processos semelhantes e ajudar a evitar erros de configuração ao inserir as informações da conta.

## AFTsuporta personalização automatizada para contas compartilhadas da AWS Control Tower

27 de maio de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

O Account Factory for Terraform (AFT) agora pode personalizar e atualizar programaticamente qualquer uma das suas contas gerenciadas pela AWS Control Tower, incluindo a conta de gerenciamento, a conta de auditoria e a conta de arquivamento de registros, junto com suas contas inscritas. Você pode centralizar a personalização da sua conta e o gerenciamento de atualizações e, ao mesmo tempo, proteger a segurança das configurações da sua conta, porque você define a função que executa o trabalho.

A AWSAFTExecutionfunção existente agora implanta personalizações em todas as contas. Você pode configurar IAM permissões com limites que limitam o acesso à AWSAFTExecutionfunção de acordo com seus requisitos comerciais e de segurança. Você também pode delegar programaticamente as permissões de personalização aprovadas nessa função para usuários confiáveis. Como prática recomendada, recomendamos que você restrinja as permissões às necessárias para implantar as personalizações necessárias.

AFTagora cria a nova AWSAFTServicefunção para implantar AFT recursos em todas as contas gerenciadas, incluindo as contas compartilhadas e a conta de gerenciamento. Anteriormente, os recursos eram distribuídos pela AWSAFTExecutionfunção.

As contas compartilhadas e de gerenciamento da AWS Control Tower não são provisionadas pela fábrica de contas, portanto, elas não têm produtos provisionados correspondentes no AWS Service Catalog. Portanto, você não pode atualizar as contas compartilhadas e de gerenciamento no Service Catalog.

## Operações simultâneas para todos os controles opcionais

18 de maio de 2022

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora suporta operações simultâneas para controles preventivos, bem como para controles de detetive.

Com esse novo recurso, qualquer controle opcional agora pode ser aplicado ou removido simultaneamente, melhorando assim a facilidade de uso e o desempenho de todos os controles opcionais. Você pode ativar vários controles opcionais sem esperar que as operações de controle individuais sejam concluídas. Os únicos horários restritos são quando a AWS Control Tower está no processo de configuração da landing zone ou ao estender a governança a uma nova organização.

Funcionalidade suportada para controles preventivos:

- Aplique e remova diferentes controles preventivos na mesma UO.
- Aplique e remova diferentes controles preventivos em diferentesOUs, simultaneamente.
- Aplique e remova o mesmo controle preventivo em váriosOUs, simultaneamente.
- Você pode aplicar e remover quaisquer controles preventivos e de detetive simultaneamente.

Você pode experimentar essas melhorias de controle simultâneo em todas as versões lançadas do AWS Control Tower.

Quando você aplica controles preventivos ao aninhadoOUs, os controles preventivos afetam todas as contas e estão OUs aninhadas na OU de destino, mesmo que essas contas não OUs estejam registradas na AWS Control Tower. Os controles preventivos são implementados usando as Políticas de Controle de Serviços (SCPs), que fazem parte do AWS Organizations. Os controles de detetive são implementados usando AWS Config regras. As proteções permanecem em vigor à medida que você cria novas contas ou faz alterações em suas contas existentes, e o AWS Control Tower fornece um relatório resumido de como cada conta está em conformidade com suas políticas habilitadas. Para obter uma lista completa dos controles disponíveis, consulte a biblioteca de controles da AWS Control Tower.

## Contas de segurança e registro existentes

16 de maio de 2022

(Disponível durante a configuração inicial.)

AWSO Control Tower agora oferece a opção de especificar um existente AWS conta como uma conta de segurança ou de registro da AWS Control Tower, durante o processo inicial de configuração da landing zone. Essa opção elimina a necessidade de a AWS Control Tower criar contas novas e compartilhadas. A conta de segurança, chamada de conta de auditoria por padrão, é uma conta restrita que dá às equipes de segurança e conformidade acesso a todas as contas em sua landing zone. A conta de registro, chamada de conta do Arquivo de registros por padrão, funciona como um repositório. Ele armazena registros de API atividades e configurações de recursos de todas as contas em sua landing zone.

Ao trazer suas contas de segurança e registro existentes, é mais fácil estender a governança da AWS Control Tower às suas organizações existentes ou migrar para a AWS Control Tower de uma landing zone alternativa. A opção de usar contas existentes é exibida durante a configuração inicial

da landing zone. Inclui verificações durante o processo de configuração, que garantem a implantação bem-sucedida. AWSA Control Tower implementa as funções e controles necessários em suas contas existentes. Ele não remove nem mescla nenhum recurso ou dado existente nessas contas.

Limitação: Se você planeja trazer os existentes AWS contas na AWS Control Tower como contas de auditoria e arquivamento de registros, e se essas contas já existirem AWS Config recursos, você deve excluir os existentes AWS Config recursos antes que você possa inscrever as contas na AWS Control Tower.

## AWSVersão 2.9 da zona de pouso da Control Tower

22 de abril de 2022

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 2.9. Para obter informações, consulteAtualize sua landing zone)

AWSA versão 2.9 da zona de pouso do Control Tower atualiza o encaminhador de notificações Lambda para usar o tempo de execução do Python versão 3.9. Essa atualização aborda a descontinuação da versão 3.6 do Python, planejada para julho de 2022. Para obter as informações mais recentes, consulte a página de descontinuação do Python.

## AWSVersão 2.8 da zona de pouso da Control Tower

10 de fevereiro de 2022

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 2.8. Para obter informações, consulteAtualize sua landing zone)

AWSA versão 2.8 da zona de pouso do Control Tower adiciona funcionalidade que se alinha às atualizações recentes do AWS Melhores práticas básicas de segurança.

Nesta versão:

- O registro de acesso é configurado para o bucket de log de acesso na conta do Log Archive, para acompanhar o acesso ao bucket de log de acesso existente do S3.
- O suporte para a política de ciclo de vida foi adicionado. O log de acesso do bucket de log de acesso existente do S3 está definido para um tempo de retenção padrão de 10 anos.
- Além disso, esta versão atualiza AWS o Control Tower para usar o AWS Função vinculada ao serviço (SLR) fornecida por AWS Config, em todas as contas gerenciadas (não incluindo a conta de gerenciamento), para que você possa configurar e gerenciar as regras do Config de

acordo com as mesmas AWS Config melhores práticas. Os clientes que não fizerem o upgrade continuarão usando sua função atual.

- Esta versão simplifica o processo de KMS configuração da AWS Control Tower para criptografia AWS Config dados e melhora as mensagens de status relacionadas CloudTrail.
- A versão inclui uma atualização do controle de negação da região, para permitir a entrada do `route53-application-recovery` recursous-west-2.
- Atualização: em 15 de fevereiro de 2022, removemos a fila de letras mortas para AWS Funções do Lambda.

Outros detalhes:

- Se você descomissionar sua landing zone, o AWS Control Tower não removerá o AWS Config função vinculada ao serviço.
- Se você desprovisionar uma conta do Account Factory, a AWS Control Tower não removerá a AWS Config função vinculada ao serviço.

Para atualizar sua zona de pouso para 2.8, navegue até a página de configurações da zona de pouso, selecione a versão 2.8 e escolha Atualizar. Depois de atualizar sua landing zone, você deve atualizar todas as contas que são governadas pela AWS Control Tower, conforme indicado emGerenciamento de atualizações de configuração no AWS Control Tower.

## Janeiro a dezembro de 2021

Em 2021, a AWS Control Tower lançou as seguintes atualizações:

- Capacidade de negação da região
- Recursos de residência de dados
- AWSControl Tower apresenta o provisionamento e a personalização de contas do Terraform
- Novo evento de ciclo de vida disponível
- AWSO Control Tower permite o aninhamento OUs
- Detective: controle simultâneo
- Duas novas regiões disponíveis
- Desseleção de região
- AWSO Control Tower funciona com AWS Sistemas de gerenciamento de chaves

- Controles renomeados, funcionalidade inalterada
- AWSA Control Tower escaneia SCPs diariamente para verificar se há desvio
- Nomes OUs e contas personalizados
- AWSVersão 2.7 da zona de pouso da Control Tower
- Três novos AWS Regiões disponíveis
- Governe somente regiões selecionadas
- AWSA Control Tower agora estende a governança para a existente OUs em seu AWS organizações
- AWSA Control Tower fornece atualizações de contas em massa

## Capacidade de negação da região

30 de novembro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower.)

AWSO Control Tower agora fornece recursos de negação de região, que ajudam você a limitar o acesso a AWS serviços e operações para contas inscritas em seu ambiente AWS Control Tower. O recurso de negação de região complementa os recursos existentes de seleção e desseleção de região no AWS Control Tower. Juntos, esses recursos ajudam você a lidar com questões regulatórias e de conformidade, ao mesmo tempo em que equilibram os custos associados à expansão para outras regiões.

Por exemplo, AWS clientes na Alemanha podem negar o acesso a AWS serviços em regiões fora da região de Frankfurt. Você pode selecionar regiões restritas durante o processo de configuração da AWS Control Tower ou na página de configurações da zona de pouso. O recurso de negação de região está disponível quando você atualiza sua versão da zona de pouso do AWS Control Tower. Selecionar AWS os serviços estão isentos dos recursos de negação da região. Para saber mais, consulte Configurar o controle de negação de região.

## Recursos de residência de dados

30 de novembro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora oferece controles específicos para ajudar a garantir que todos os dados do cliente para os quais você envie AWS os serviços estão localizados somente no AWS Regiões

que você especifica. Você pode selecionar o AWS Região ou regiões nas quais os dados de seus clientes são armazenados e processados. Para obter uma lista completa de AWS Regiões em que AWS o Control Tower está disponível, consulte o AWS Tabela de regiões.

Para controle granular, você pode aplicar controles adicionais, como Proibir conexões da Amazon Virtual Private Network (VPN) ou Proibir o acesso à Internet para uma instância da Amazon. VPC Você pode ver o status de conformidade dos controles no console do AWS Control Tower. Para obter uma lista completa dos controles disponíveis, consulte a biblioteca de controles da AWS Control Tower.

## AWSControl Tower apresenta o provisionamento e a personalização de contas do Terraform

29 de novembro de 2021

(Atualização opcional para a zona de pouso da AWS Control Tower)

Agora você pode usar o Terraform para provisionar e atualizar contas personalizadas por meio da AWS Control Tower, com AWS o Control Tower Account Factory for Terraform (). AFT

AFTfornece um único pipeline de infraestrutura como código (IaC) do Terraform, que provisiona contas gerenciadas pela AWS Control Tower. As personalizações durante o provisionamento ajudam a cumprir suas políticas comerciais e de segurança, antes de você fornecer as contas aos usuários finais.

O pipeline AFT automatizado de criação de contas monitora até que o provisionamento da conta seja concluído e, em seguida, continua, acionando módulos adicionais do Terraform que aprimoram a conta com as personalizações necessárias. Como parte adicional do processo de personalização, você pode configurar o pipeline para instalar seus próprios módulos personalizados do Terraform e pode optar por adicionar qualquer uma das opções de AFT recursos, fornecidas pelo AWS para personalizações comuns.

Comece a usar o AWS Control Tower Account Factory for Terraform seguindo as etapas fornecidas no Guia do usuário do AWS Control Tower e fazendo o download AFT para sua instância do Terraform. Implante AWS o Control Tower Account Factory para Terraform () AFT AFToferece suporte às distribuições Terraform Cloud, Terraform Enterprise e Terraform Open Source.

## Novo evento de ciclo de vida disponível

18 de novembro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

O `PrecheckOrganizationalUnit` evento registra se algum recurso impede o sucesso da tarefa de governança Extend, incluindo recursos aninhadosOUs. Para obter mais informações, consulte `PrecheckOrganizationalUnit`.

## AWSO Control Tower permite o aninhamento OUs

16 de novembro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora permite que você inclua o aninhado OUs como parte da sua landing zone.

AWSO Control Tower fornece suporte para unidades organizacionais aninhadas (OUs), permitindo que você organize contas em vários níveis hierárquicos e aplique controles preventivos hierarquicamente. Você pode registrar OUs contendo aninhadoOUs, criar e registrar OUs como pai OUs e ativar controles em qualquer OU registrada, independentemente da profundidade. Para oferecer suporte a essa funcionalidade, o console mostra o número de contas controladas e. OUs

Com o nestedOUs, você pode alinhar sua AWS Control Tower OUs ao AWS estratégia de várias contas, e você pode reduzir o tempo necessário para ativar controles em váriasOUs, aplicando controles no nível da OU principal.

Considerações importantes

1. Você pode registrar uma OU existente em vários níveis OUs no AWS Control Tower, uma OU por vez, começando com a OU de nível superior e depois descendo pela árvore. Para obter mais informações, consulte Expandir de uma estrutura de OU plana para uma estrutura de OU aninhada.
2. As contas diretamente em uma OU registrada são registradas automaticamente. As contas mais abaixo na árvore podem ser registradas registrando sua OU principal imediata.
3. Os controles preventivos (SCPs) são herdados automaticamente na hierarquia; SCPs aplicados ao pai são herdados por todos os aninhados. OUs
4. Controles de detetive (AWS Config (regras) são NOT herdadas automaticamente.
5. A conformidade com os controles de detetive é relatada por cada UO.
6. SCPA deriva em uma OU afeta todas as contas e OUs abaixo dela.
7. Você não pode criar um novo OUs aninhado na OU de segurança (OU principal).

## Detective: controle simultâneo

5 de novembro de 2021

(Atualização opcional para a zona de pouso da AWS Control Tower)

AWSOs controles de detetive da Control Tower agora oferecem suporte a operações simultâneas para controles de detetive, melhorando a facilidade de uso e o desempenho. Você pode ativar vários controles de detetive sem esperar que as operações de controle individuais sejam concluídas.

Funcionalidade suportada:

- Ative diferentes controles de detecção na mesma UO (por exemplo, Detecte se MFA o usuário raiz está habilitado e Detecte se o acesso público de gravação aos buckets do Amazon S3 é permitido).
- Ative diferentes controles de detetive em diferentesOUs, simultaneamente.
- As mensagens de erro do Guardrail foram aprimoradas para fornecer orientação adicional para operações de concorrência de controle suportadas.

Não suportado nesta versão:

- Não OUs há suporte para ativar o mesmo controle de detetive em vários ao mesmo tempo.
- A simultaneidade de controle preventivo não é suportada.

Você pode experimentar as melhorias simultâneas do controle de detetive em todas as versões do AWS Control Tower. É recomendável que os clientes que ainda não usam a versão 2.7 realizem uma atualização da landing zone para aproveitar outros recursos, como seleção e desseleção de regiões, que estão disponíveis na versão mais recente.

## Duas novas regiões disponíveis

29 de julho de 2021

(Atualização necessária para a zona de pouso da AWS Control Tower)

AWSO Control Tower agora está disponível em duas versões adicionais AWS Regiões: América do Sul (São Paulo) e Europa (Paris). Esta atualização expande a disponibilidade do AWS Control Tower para 15 AWS Regiões.

Se você é novo no AWS Control Tower, pode iniciá-lo imediatamente em qualquer uma das regiões suportadas. Durante o lançamento, você pode selecionar as regiões nas quais deseja que a AWS Control Tower construa e controle seu ambiente de várias contas.

Se você já tem um ambiente de AWS Control Tower e deseja estender ou remover os recursos de governança da AWS Control Tower em uma ou mais regiões suportadas, acesse a página Landing Zone Settings no painel da AWS Control Tower e selecione as Regiões. Depois de atualizar sua landing zone, você deve então atualizar todas as contas que são administradas pela AWS Control Tower.

## Desseleção de região

29 de julho de 2021

(Atualização opcional para a zona de pouso da AWS Control Tower)

AWSA desseleção da região da Control Tower aprimora sua capacidade de gerenciar a área geográfica dos recursos da AWS Control Tower. Você pode desmarcar regiões que você não gostaria mais de governar pela AWS Control Tower. Esse recurso oferece a capacidade de abordar questões regulatórias e de conformidade e, ao mesmo tempo, equilibrar os custos associados à expansão para outras regiões.

A desseleção da região está disponível quando você atualiza sua versão da zona de pouso do AWS Control Tower.

Quando você usa o Account Factory para criar uma nova conta ou inscrever uma conta de membro preexistente, ou quando seleciona Extend Governance para inscrever contas em uma unidade organizacional preexistente, a Control Tower implanta seus recursos de governança, que incluem registro, monitoramento e AWS controles centralizados, nas regiões escolhidas nas contas. A opção de desmarcar uma região e remover a governança da AWS Control Tower dessa região remove essa funcionalidade de governança, mas não inibe a capacidade de implantação dos usuários AWS recursos ou cargas de trabalho nessas regiões.

## AWSO Control Tower funciona com AWS Sistemas de gerenciamento de chaves

28 de julho de 2021

(Atualização opcional para a zona de pouso da AWS Control Tower)

AWSO Control Tower oferece a opção de usar um AWS Serviço de gerenciamento de chaves (AWS KMS) chave. Uma chave é fornecida e gerenciada por você para proteger os serviços que a AWS Control Tower implanta, incluindo AWS CloudTrail, AWS Config e os dados associados do Amazon S3. AWS KMScriptografia é um nível aprimorado de criptografia em relação à criptografia SSE -S3 que a AWS Control Tower usa por padrão.

A integração do AWS KMSo suporte ao AWS Control Tower está alinhado com o AWS Melhores práticas básicas de segurança, que recomendam uma camada adicional de segurança para seus arquivos de log confidenciais. Você deve usar AWS KMS—chaves gerenciadas (SSE-KMS) para criptografia em repouso. AWS KMSo suporte à criptografia está disponível quando você configura uma nova zona de pouso ou quando você atualiza sua zona de pouso existente da AWS Control Tower.

Para configurar essa funcionalidade, você pode selecionar KMSKey Configuration durante a configuração inicial da landing zone. Você pode escolher uma KMS chave existente ou selecionar um botão que o direcione para o AWS KMSconsole para criar um novo. Você também tem a flexibilidade de mudar da criptografia padrão para SSE - KMS ou para uma KMS chave diferenteSSE.

Para uma zona de pouso existente da AWS Control Tower, você pode realizar uma atualização para começar a usar AWS KMSchaves.

## Controles renomeados, funcionalidade inalterada

26 de julho de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSA Control Tower está revisando certos nomes e descrições de controle para melhor refletir as intenções políticas do controle. Os nomes e descrições revisados ajudam você a entender de forma mais intuitiva as formas pelas quais os controles incorporam as políticas de suas contas. Por exemplo, alteramos parte dos nomes dos controles de detetive de “Não permitir” para “Detectar” porque o controle de detetive em si não interrompe uma ação específica, ele só detecta violações de políticas e fornece alertas por meio do painel.

A funcionalidade de controle, a orientação e a implementação permanecem inalteradas. Somente os nomes e descrições dos controles foram revisados.

# AWSA Control Tower escaneia SCPs diariamente para verificar se há desvio

11 de maio de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora realiza escaneamentos automatizados diários de seu gerente SCPs para verificar se os controles correspondentes foram aplicados corretamente e se não foram desviados. Se um escaneamento descobrir um desvio, você receberá uma notificação. AWSO Control Tower envia apenas uma notificação por problema de deriva, portanto, se sua landing zone já estiver em um estado de deriva, você não receberá notificações adicionais a menos que um novo item de deriva seja encontrado.

# Nomes OUs e contas personalizados

16 de abril de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora permite que você personalize o nome da sua landing zone. Você pode manter os nomes que a AWS Control Tower recomenda para as unidades organizacionais (OUs) e as contas principais, ou pode modificá-los durante o processo inicial de configuração da landing zone.

Os nomes padrão que o AWS Control Tower fornece para as contas principais OUs e as contas principais correspondem ao AWS orientação sobre as melhores práticas para várias contas. No entanto, se sua empresa tiver políticas de nomenclatura específicas ou se você já tiver uma OU ou conta existente com o mesmo nome recomendado, a nova funcionalidade de nomenclatura de conta e UO oferece a flexibilidade de lidar com essas restrições.

Separadamente dessa mudança de fluxo de trabalho durante a configuração, a OU anteriormente conhecida como Core OU agora é chamada de Security OU, e a OU anteriormente conhecida como Custom OU agora é chamada de Sandbox OU. Fizemos essa alteração para melhorar nosso alinhamento com o geral AWS orientação de melhores práticas para nomenclatura.

Novos clientes verão esses novos nomes de UO. Os clientes existentes continuarão vendo os nomes originais delesOUs. Você pode encontrar algumas inconsistências na nomenclatura da UO enquanto atualizamos nossa documentação para os novos nomes.

Para começar a usar o AWS Control Tower a partir do AWS Management Console, acesse o console AWS Control Tower e selecione Configurar landing zone no canto superior direito. Para obter informações adicionais, você pode ler sobre o planejamento da sua landing zone da AWS Control Tower.

## AWSVersão 2.7 da zona de pouso da Control Tower

8 de abril de 2021

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 2.7. Para obter informações, consulteAtualize sua landing zone)

Com a versão 2.7 do AWS Control Tower, a AWS Control Tower introduz quatro novos controles preventivos obrigatórios de arquivamento de registros que implementam políticas somente nos recursos da AWS Control Tower. Ajustamos a orientação de quatro controles existentes do Log Archive de obrigatórios para eletivos, porque eles definem políticas para recursos fora da AWS Control Tower. Essa mudança e expansão de controle oferecem a capacidade de separar a governança do Log Archive para recursos dentro da AWS Control Tower da governança de recursos fora da AWS Control Tower.

Os quatro controles alterados podem ser usados em conjunto com os novos controles obrigatórios para fornecer governança a um conjunto mais amplo de AWS Arquivos de log. Os ambientes existentes da AWS Control Tower manterão esses quatro controles alterados ativados automaticamente, para manter a consistência do ambiente; no entanto, esses controles eletivos agora podem ser desativados. Os novos ambientes da AWS Control Tower devem habilitar todos os controles eletivos. Os ambientes existentes devem desativar os controles anteriormente obrigatórios antes de adicionar criptografia aos buckets do Amazon S3 que não são implantados pela AWS Control Tower.

Novos controles obrigatórios:

- Proibir alterações na configuração de criptografia para buckets S3 criados pela AWS Control Tower no Log Archive
- Proibir alterações na configuração de registro para buckets S3 criados pela AWS Control Tower no Log Archive
- Proibir alterações na política de buckets S3 criados pela AWS Control Tower no Log Archive
- Proibir alterações na configuração do ciclo de vida dos buckets S3 criados pela AWS Control Tower no Log Archive

A orientação mudou de obrigatória para eletiva:

- Proibir alterações na configuração de criptografia para todos os buckets do Amazon S3 [Anteriormente: Ativar criptografia em repouso para arquivamento de registros]
- Proibir alterações na configuração de registro para todos os buckets do Amazon S3 [Anteriormente: habilitar o registro de acesso para arquivamento de registros]
- Proibir alterações na política de bucket para todos os buckets do Amazon S3 [Anteriormente: Proibir alterações de política no arquivamento de registros]
- Proibir alterações na configuração do ciclo de vida de todos os buckets do Amazon S3 [Anteriormente: defina uma política de retenção para o arquivamento de registros]

AWSA versão 2.7 do Control Tower inclui alterações no esquema da zona de pouso da AWS Control Tower que podem causar incompatibilidade com versões anteriores após a atualização para a 2.7.

- Em particular, a versão 2.7 do AWS Control Tower é ativada `BlockPublicAccess` automaticamente em buckets S3 implantados pela Control TowerAWS. Você pode desativar esse padrão se sua carga de trabalho exigir acesso em várias contas. Para obter mais informações sobre o que acontece com a `BlockPublicaccess` opção ativada, consulte Bloqueio do acesso público ao seu armazenamento no Amazon S3.
- AWSA versão 2.7 do Control Tower inclui um requisito paraHTTPS. Todas as solicitações enviadas aos buckets do S3 implantados pela AWS Control Tower devem usar a camada de soquete segura (). SSL Somente HTTPS solicitações podem ser aprovadas. Se você usa HTTP (semSSL) como um endpoint para enviar as solicitações, essa alteração gera um erro de acesso negado, o que pode interromper seu fluxo de trabalho. Essa alteração não pode ser revertida após a atualização 2.7 em sua landing zone.

  Recomendamos que você altere suas solicitações para usar TLS em vez deHTTP.

## Três novos AWS Regiões disponíveis

8 de abril de 2021

(Atualização necessária para a zona de pouso da AWS Control Tower)

AWSO Control Tower está disponível em três versões adicionais AWS Regiões: região Ásia-Pacífico (Tóquio), região Ásia-Pacífico (Seul) e região Ásia-Pacífico (Mumbai). É necessária uma atualização da landing zone para a versão 2.7 para expandir a governança nessas regiões.

Sua landing zone não é expandida automaticamente para essas regiões quando você realiza a atualização para a versão 2.7. Você deve visualizá-las e selecioná-las na tabela Regiões para inclusão.

## Governe somente regiões selecionadas

19 de fevereiro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSA seleção da região da Control Tower oferece melhor capacidade de gerenciar a área geográfica dos recursos da AWS Control Tower. Para expandir o número de regiões nas quais você hospeda AWS recursos ou cargas de trabalho — por motivos de conformidade, regulamentação, custo ou outros — agora você pode selecionar as regiões adicionais a serem governadas.

A seleção de região está disponível quando você configura uma nova zona de pouso ou atualiza sua versão da zona de pouso da AWS Control Tower. Quando você usa o Account Factory para criar uma nova conta ou inscrever uma conta de membro preexistente, ou quando usa o Extend Governance para inscrever contas em uma unidade organizacional preexistente, a Control AWS Tower implanta seus recursos de governança de registro, monitoramento e controles centralizados nas regiões escolhidas nas contas. Para obter mais informações sobre a seleção de regiões, consulteConfigure suas regiões AWS da Control Tower.

## AWSA Control Tower agora estende a governança para a existente OUs em seu AWS organizações

28 de janeiro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

Estenda a governança às unidades organizacionais existentes (OUs) (aquelas que não estão na AWS Control Tower) a partir do console da AWS Control Tower. Com esse recurso, você pode colocar contas de alto nível OUs e incluídas sob a governança da AWS Control Tower. Para obter informações sobre como estender a governança a uma OU inteira, consulteRegistre uma unidade organizacional existente na AWS Control Tower.

Quando você registra uma OU, a AWS Control Tower executa uma série de verificações para garantir a extensão bem-sucedida da governança e a inscrição de contas na OU. Para obter mais informações sobre problemas comuns associados ao registro inicial de uma OU, consulteCausas comuns de falha durante o registro ou o novo registro.

Você também pode visitar a página do produto AWS Control Tower ou assistir YouTube a este vídeo sobre como começar a usar o AWS Control Tower for AWS Organizations.

## AWSA Control Tower fornece atualizações de contas em massa

28 de janeiro de 2021

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

Com o recurso de atualização em massa, agora você pode atualizar todas as contas em um cadastro AWS Organizations unidade organizacional (OU) contendo até 300 contas, com um único clique, no painel do AWS Control Tower. Isso é particularmente útil nos casos em que você atualiza sua zona de pouso do AWS Control Tower e também precisa atualizar suas contas inscritas para alinhá-las à versão atual da zona de pouso.

Esse recurso também ajuda você a manter suas contas atualizadas quando você atualiza sua landing zone da AWS Control Tower para expandir para novas regiões, ou quando você deseja registrar novamente uma OU para garantir que todas as contas nessa OU tenham os controles mais recentes aplicados. A atualização em massa da conta elimina a necessidade de atualizar uma conta por vez ou usar um script externo para realizar a atualização em várias contas.

Para obter informações sobre como atualizar um landing zone, consulteAtualize sua landing zone.

Para obter informações sobre como registrar ou registrar novamente uma OU, consulte. Registre uma unidade organizacional existente na AWS Control Tower

# Janeiro a dezembro de 2020

Em 2020, a AWS Control Tower lançou as seguintes atualizações:

- AWSO console Control Tower agora está vinculado ao externo AWS Config Rules
- AWSControl Tower agora disponível em outras regiões
- Atualização do guardrail
- AWSO console Control Tower mostra mais detalhes sobre contas OUs e
- Use a AWS Control Tower para configurar uma nova conta múltipla AWS ambientes em AWS Organizations
- Personalizações para a solução AWS Control Tower
- Disponibilidade geral do AWS Control Tower versão 2.3

- Provisionamento de contas em uma única etapa na Control Tower AWS
- AWSFerramenta de descomissionamento da Control Tower
- AWSNotificações de eventos do ciclo de vida da Control Tower

## AWSO console Control Tower agora está vinculado ao externo AWS Config Rules

29 de dezembro de 2020

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 2.6. Para obter informações, consulteAtualize sua landing zone)

AWSO Control Tower agora inclui um agregador em nível organizacional, que auxilia na detecção externa AWS Regras de configuração. Isso fornece visibilidade no console do AWS Control Tower para ver a existência de objetos criados externamente. AWS Regras de configuração, além dessas AWS Regras de configuração criadas pela AWS Control Tower. O agregador permite que o AWS Control Tower detecte regras externas e forneça um link para o AWS Configure o console sem a necessidade de o AWS Control Tower ter acesso a contas não gerenciadas.

Com esse recurso, agora você tem uma visão consolidada dos controles de detetive aplicados às suas contas para poder monitorar a conformidade e determinar se precisa de controles adicionais para sua conta. Para obter informações, consulte Como a AWS Control Tower agrega AWS Config regras em contas OUs e contas não gerenciadas.

## AWSControl Tower agora disponível em outras regiões

18 de novembro de 2020

(Atualização necessária para a zona de pouso do AWS Control Tower para a versão 2.5. Para obter informações, consulteAtualize sua landing zone)

AWSO Control Tower agora está disponível em mais 5 AWS Regiões:

- Região Ásia-Pacífico (Singapura)
- Região Europa (Frankfurt)
- Região Europa (Londres)
- Região Europa (Estocolmo)
- Região Canadá (Central)

A adição desses 5 AWS Regions é a única alteração introduzida na versão 2.5 do AWS Control Tower.

AWSA Control Tower também está disponível nas regiões Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Europa (Irlanda) e Ásia-Pacífico (Sydney). Com este lançamento, o AWS Control Tower está agora disponível em 10 AWS Regiões.

Essa atualização da landing zone inclui todas as regiões listadas e não pode ser desfeita. Depois de atualizar sua landing zone para a versão 2.5, você deve atualizar manualmente todas as contas inscritas para que a AWS Control Tower governe nas 10 suportadas AWS Regiões. Para ter mais informações, consulte Configure suas regiões AWS da Control Tower.

## Atualização do guardrail

8 de outubro de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

Uma versão atualizada foi lançada para o controle obrigatórioAWS-GR_IAM_ROLE_CHANGE_PROHIBITED.

Essa alteração no controle é necessária porque as contas que estão sendo inscritas automaticamente no AWS Control Tower devem ter a AWSControlTowerExecution função ativada. A versão anterior do controle impede que essa função seja criada.

Para obter mais informações, consulte Não permitir alterações no AWS IAMFunções configuradas pela AWS Control Tower e AWS CloudFormationno Guia de referência dos AWS Control Tower Controls.

## AWSO console Control Tower mostra mais detalhes sobre contas OUs e

22 de julho de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

Você pode ver suas organizações e contas que não estão inscritas no AWS Control Tower, juntamente com organizações e contas que estão inscritas.

No console do AWS Control Tower, você pode ver mais detalhes sobre seu AWS contas e unidades organizacionais (OUs). A página Contas agora lista todas as contas em sua organização, independentemente da OU ou do status de inscrição na AWS Control Tower. Agora você pode pesquisar, classificar e filtrar em todas as tabelas.

## Use a AWS Control Tower para configurar uma nova conta múltipla AWS ambientes em AWS Organizations

22 de abril de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWS Organizations Agora, os clientes podem usar o AWS Control Tower para gerenciar unidades organizacionais (OUs) e contas recém-criadas, aproveitando esses novos recursos:

- Existente AWS Organizations agora, os clientes podem configurar uma nova landing zone para novas unidades organizacionais (OUs) em sua conta de gerenciamento existente. Você pode criar novas contas OUs na AWS Control Tower e criar novas contas naquelas OUs com governança da AWS Control Tower.
- AWS Organizations os clientes podem inscrever contas existentes usando o processo de inscrição de contas ou por meio de scripts.

AWSO Control Tower fornece um serviço de orquestração que usa outros AWS serviços. Ele foi projetado para organizações com várias contas e equipes que buscam a maneira mais fácil de configurar suas contas múltiplas novas ou existentes AWS meio ambiente e governo em grande escala. Com uma organização governada pela AWS Control Tower, os administradores de nuvem sabem que as contas na organização estão em conformidade com as políticas estabelecidas. Os construtores se beneficiam porque podem provisionar novos AWS contas rapidamente, sem preocupações indevidas com a conformidade.

Para obter informações sobre como configurar uma landing zone, consultePlaneje sua zona de pouso da AWS Control Tower. Você também pode visitar a página do produto AWS Control Tower ou assistir YouTube a este vídeo sobre como começar a usar o AWS Control Tower for AWS Organizations.

Além dessa alteração, o recurso de provisionamento rápido de contas no AWS Control Tower foi renomeado para Enroll account. Agora permite a inscrição de pessoas existentes AWS contas, bem como criação de novas contas. Para obter mais informações, consulte Inscrever uma conta existente.

## Personalizações para a solução AWS Control Tower

17 de março de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora inclui uma nova implementação de referência que facilita a aplicação de modelos e políticas personalizados à sua landing zone da AWS Control Tower.

Com personalizações para o AWS Control Tower, você pode usar AWS CloudFormation modelos para implantar novos recursos em contas novas e existentes em sua organização. Você também pode aplicar políticas de controle de serviço personalizadas (SCPs) a essas contas, além das SCPs já fornecidas pela AWS Control Tower. As personalizações do pipeline da AWS Control Tower se integram aos eventos e notificações do ciclo de vida da AWS Control Tower (Eventos de ciclo de vida no AWS Control Tower) para garantir que as implantações de recursos permaneçam sincronizadas com sua landing zone.

A documentação de implantação dessa arquitetura de solução AWS Control Tower está disponível por meio do AWS Página da web de soluções.

## Disponibilidade geral do AWS Control Tower versão 2.3

5 de março de 2020

(Atualização necessária para a landing zone da AWS Control Tower. Para obter informações, consulteAtualize sua landing zone.)

AWSA Control Tower agora está disponível na Ásia-Pacífico (Sydney) AWS Região, além das regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda). A adição da região Ásia-Pacífico (Sydney) é a única alteração introduzida na versão 2.3 do AWS Control Tower.

Se você não usou o AWS Control Tower anteriormente, você pode iniciá-lo hoje em qualquer uma das regiões suportadas. Se você já estiver usando a AWS Control Tower e quiser estender seus recursos de governança para a região Ásia-Pacífico (Sydney) em suas contas, acesse a página Configurações no painel da AWS Control Tower. A partir daí, atualize sua landing zone para a versão mais recente. Em seguida, atualize suas contas individualmente.

> **Note**
>
> Atualizar sua landing zone não atualiza automaticamente suas contas. Se você tiver mais do que algumas contas, as atualizações necessárias podem ser demoradas. Por esse motivo, recomendamos que você evite expandir sua zona de pouso do AWS Control Tower para regiões nas quais não exija que suas cargas de trabalho sejam executadas.

Para obter informações sobre o comportamento esperado dos controles de detetive como resultado de uma implantação em uma nova região, consulte Configurar suas regiões do AWS Control Tower.

## Provisionamento de contas em uma única etapa na Control Tower AWS

2 de março de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora oferece suporte ao provisionamento de contas em uma única etapa por meio do console da AWS Control Tower. Esse recurso permite provisionar novas contas a partir do console do AWS Control Tower.

Para usar o formulário simplificado, navegue até Account Factory no console AWS Control Tower e escolha Provisionamento rápido de contas. AWSA Control Tower atribui o mesmo endereço de e-mail à conta provisionada e ao usuário de login único (IAMIdentity Center) criado para a conta. Se você precisar que esses dois endereços de e-mail sejam diferentes, você deverá provisionar sua conta por meio do Service Catalog.

Atualize as contas que você cria por meio do provisionamento rápido de contas usando o Service Catalog e a fábrica de contas AWS Control Tower, assim como as atualizações em qualquer outra conta.

> **Note**
>
> Em abril de 2020, o recurso de provisionamento rápido de contas foi renomeado para Inscrever conta. Em junho de 2022, a capacidade de criar e atualizar contas no console AWS Control Tower foi separada da capacidade de se inscrever. AWS contas. Para obter mais informações, consulte Inscrever uma conta existente.

## AWSFerramenta de descomissionamento da Control Tower

28 de fevereiro de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora oferece suporte a uma ferramenta de descomissionamento automatizado para ajudá-lo a limpar os recursos alocados pela Control TowerAWS. Se você não pretende mais usar o AWS Control Tower em sua empresa ou se precisar de uma grande

redistribuição de seus recursos organizacionais, talvez queira limpar os recursos criados quando você configurou inicialmente sua landing zone.

Para descomissionar sua landing zone usando um processo que é principalmente automatizado, entre em contato com AWS Support para obter assistência com as etapas adicionais necessárias. Para obter mais informações sobre o descomissionamento, consulte. Passo a passo: Descomissione uma zona de pouso do AWS Control Tower

## AWSNotificações de eventos do ciclo de vida da Control Tower

22 de janeiro de 2020

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSA Control Tower anuncia a disponibilidade de notificações de eventos do ciclo de vida. Um evento de ciclo de vida marca a conclusão de uma ação da AWS Control Tower que pode alterar o estado dos recursos, como unidades organizacionais (OUs), contas e controles criados e gerenciados pela AWS Control Tower. Os eventos do ciclo de vida são registrados como AWS CloudTrail eventos e entregues à Amazon EventBridge como eventos.

AWSO Control Tower registra os eventos do ciclo de vida ao concluir as seguintes ações que podem ser realizadas usando o serviço: criar ou atualizar uma landing zone; criar ou excluir uma OU; ativar ou desativar um controle em uma OU; e usar o account factory para criar uma nova conta ou mover uma conta para outra OU.

AWSA Control Tower usa vários AWS serviços para criar e administrar uma conta múltipla de melhores práticas AWS meio ambiente. Pode levar vários minutos para que uma ação da AWS Control Tower seja concluída. Você pode rastrear eventos do ciclo de vida nos CloudTrail registros para verificar se a ação original da AWS Control Tower foi concluída com êxito. Você pode criar uma EventBridge regra para notificá-lo quando CloudTrail registrar um evento do ciclo de vida ou para acionar automaticamente a próxima etapa em seu fluxo de trabalho de automação.

# Janeiro a dezembro de 2019

De 1º de janeiro a 31 de dezembro de 2019, a AWS Control Tower lançou as seguintes atualizações:

- Disponibilidade geral do AWS Control Tower versão 2.2
- Novos controles eletivos na AWS Control Tower
- Novos controles de detetive na AWS Control Tower

- AWSA Control Tower aceita endereços de e-mail para contas compartilhadas com domínios diferentes da conta de gerenciamento
- Disponibilidade geral do AWS Control Tower versão 2.1

## Disponibilidade geral do AWS Control Tower versão 2.2

13 de novembro de 2019

(Atualização necessária para a landing zone da AWS Control Tower. Para obter informações, consulteAtualize sua landing zone.)

AWSA versão 2.2 do Control Tower fornece três novos controles preventivos que evitam desvios nas contas:

- Proibir alterações nos grupos de log do Amazon CloudWatch Logs configurados pela AWS Control Tower
- Não permitir a exclusão de AWS Config Autorizações de agregação criadas pela AWS Control Tower
- Não permitir a exclusão do arquivo de log

Um controle é uma regra de alto nível que fornece governança contínua para sua vida geral AWS meio ambiente. Quando você cria sua zona de pouso da AWS Control Tower, a zona de pouso e todas as unidades organizacionais (OUs), contas e recursos estão em conformidade com as regras de governança impostas pelos controles escolhidos. Conforme você e os membros da sua organização usam o landing zone, mudanças (acidentais ou intencionais) nesse status de conformidade podem ocorrer. A detecção de desvios ajuda a identificar recursos que precisam de alterações ou atualizações de configuração para resolver o desvio. Para obter mais informações, consulte Detecte e resolva desvios na AWS Control Tower.

## Novos controles eletivos na AWS Control Tower

05 de setembro de 2019

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora inclui os quatro novos controles eletivos a seguir:

- Proibir ações de exclusão em buckets do Amazon S3 sem MFA

- Proibir alterações na configuração de replicação para buckets do Amazon S3
- Proibir ações como usuário root
- Proibir a criação de chaves de acesso para o usuário root

Um controle é uma regra de alto nível que fornece governança contínua para sua vida geral AWS meio ambiente. As proteções permitem que você expresse suas intenções políticas. Para obter mais informações, consulte Sobre os controles na AWS Control Tower.

## Novos controles de detetive na AWS Control Tower

25 de agosto de 2019

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

AWSO Control Tower agora inclui os seguintes oito novos controles de detetive:

- Detecte se o versionamento para buckets do Amazon S3 está ativado
- Detecte se MFA está habilitado para IAM usuários do AWS Console
- Detecte se MFA está habilitado para IAM usuários
- Detecte se a EBS otimização da Amazon está habilitada para EC2 instâncias da Amazon
- Detecte se EBS os volumes da Amazon estão conectados às EC2 instâncias da Amazon
- Detecte se o acesso público às instâncias do RDS banco de dados da Amazon está ativado
- Detecte se o acesso público aos snapshots do RDS banco de dados da Amazon está ativado
- Detecte se a criptografia de armazenamento está habilitada para instâncias RDS de banco de dados da Amazon

Um controle é uma regra de alto nível que fornece governança contínua para sua vida geral AWS meio ambiente. Um controle de detetive detecta a não conformidade de recursos em suas contas, como violações de políticas, e fornece alertas por meio do painel. Para obter mais informações, consulte Sobre os controles na AWS Control Tower.

## AWSA Control Tower aceita endereços de e-mail para contas compartilhadas com domínios diferentes da conta de gerenciamento

01 de agosto de 2019

(Nenhuma atualização é necessária para a landing zone da AWS Control Tower)

No AWS Control Tower, agora você pode enviar endereços de e-mail para contas compartilhadas (arquivo de registros e membro de auditoria) e contas secundárias (vendidas usando a fábrica de contas) cujos domínios são diferentes do endereço de e-mail da conta de gerenciamento. Esse recurso está disponível somente quando você cria uma nova landing zone e quando você provisiona novas contas infantis.

## Disponibilidade geral do AWS Control Tower versão 2.1

24 de junho de 2019

(Atualização necessária para a landing zone da AWS Control Tower. Para obter informações, consulte Atualizar sua zona de pouso.)

AWSO Control Tower agora está disponível ao público em geral e tem suporte para uso em produção. AWSO Control Tower é destinado a organizações com várias contas e equipes que estão procurando a maneira mais fácil de configurar suas novas contas múltiplas AWS meio ambiente e governo em grande escala. Com AWS o Control Tower, você pode ajudar a garantir que as contas em sua organização estejam em conformidade com as políticas estabelecidas. Os usuários finais em equipes distribuídas podem provisionar novos AWS contas rapidamente.

Usando o AWS Control Tower, você pode configurar uma landing zone que empregue as melhores práticas, como configurar uma estrutura de várias contas usando AWS Organizations, gerenciando identidades de usuários e acesso federado com AWS IAM Identity Center, habilitando o provisionamento de contas por meio do Service Catalog e criando um arquivamento de log centralizado usando AWS CloudTrail e AWS Config.

Para uma governança contínua, você pode ativar controles pré-configurados, que são regras claramente definidas para segurança, operações e conformidade. As grades de proteção ajudam a impedir a implantação de recursos que não estão em conformidade com as políticas e monitoram continuamente a não conformidade dos recursos implantados. O painel do AWS Control Tower fornece visibilidade centralizada de um AWS ambiente, incluindo contas provisionadas, controles ativados e o status de conformidade das contas.

Você pode configurar um novo ambiente de várias contas com um único clique no console do AWS Control Tower. Não há cobranças adicionais nem compromissos iniciais de usar o AWS Control Tower. Você paga apenas por aqueles AWS serviços que você habilitou para configurar uma landing zone e implementar controles selecionados.

# Histórico do documento

- Última atualização da documentação: 30 de agosto de 2024

A tabela a seguir descreve mudanças importantes no Guia do Usuário do AWS Control Tower. Para receber notificações sobre atualizações da documentação, você pode se inscrever no RSS feed.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSO Control Tower suporta até 1.000 contas por UO | Um aumento do limite de contas por UO. | 30 de agosto de 2024 |
| AWSControl Tower adiciona seleção de versão de landing zone | Atualize ou repare sua landing zone sem mudar para a versão mais recente, se você estiver executando a versão 3.1 ou mais recente. | 15 de agosto de 2024 |
| GetControl e ListControls API operações disponíveis | Duas novas operações do Catálogo de Controle ajudam você a encontrar mais informações sobre controles. | 6 de agosto de 2024 |
| AWSO Control Tower suporta AFT e o CFCT em regiões opcionais | AFTe cFct estão disponíve is em adicionais Regiões da AWS. | 18 de julho de 2024 |
| AWSO Control Tower adiciona o `ListLandingZoneOperations` API | Um novo API que permite que você recupere operações recentes em sua landing zone. | 26 de junho de 2024 |
| AWSO Control Tower suporta até 100 operações de controle simultâneas | Um aumento da cota de operações de controle simultâneas para 100. | 20 de maio de 2024 |

| | | |
|---|---|---|
| AWSControl Tower disponível em AWS Região Oeste de Calgary (Canadá) | AWSO Control Tower está disponível na região Oeste do Canadá (Calgary). | 3 de maio de 2024 |
| AWSA Control Tower suporta ajustes de cota de autoatendimento | AWSO Control Tower é integrado com AWS Service Quotas no console. | 25 de abril de 2024 |
| A documentação dos controles foi movida para um novo guia | AWSA Control Tower publicou o Guia de referência de controles. | 21 de abril de 2024 |
| Marcando `EnabledControl` recursos em AWS CloudFormation | AWSO Control Tower suporta a adição de tags aos `EnabledControl` recursos, por meio de AWS CloudFormation modelos. | 22 de fevereiro de 2024 |
| Linha de base disponível APIs | AWSA Control Tower lançou um novo APIs para registro OUs programático. | 14 de fevereiro de 2024 |
| AWSVersão 3.3 da zona de pouso da Control Tower | AWSA versão 3.3 da zona de pouso do Control Tower está disponível. | 14 de dezembro de 2023 |
| AWSControl Tower anuncia controles para auxiliar a soberania digital | AWSA Control Tower lançou um grupo de controles para ajudar os clientes com os requisitos de soberania digital. | 27 de novembro de 2023 |
| AWSControl Tower suporta landing zone APIs | AWSO Control Tower suporta a configuração e o lançamento de zonas de pouso usando novasAPIs. | 26 de novembro de 2023 |

| | | |
|---|---|---|
| AWSO Control Tower suporta controles habilitados para marcação | AWSO Control Tower suporta controles habilitados para marcação, no console e com novosAPIs. | 10 de novembro de 2023 |
| AWSControl Tower disponível na Ásia-Pacífico (Melbourne) Região da AWS | Disponível na região Ásia-Pacífico (Melbourne). | 3 de novembro de 2023 |
| Novo controle API disponível | AWSA Control Tower lançou um novo controleAPI. | 14 de outubro de 2023 |
| AWSControl Tower lança novos controles | AWSA Control Tower lançou novos controles proativos e de detetive. | 5 de outubro de 2023 |
| AWSRelatórios da Control Tower impedem a desativação do acesso confiável | AWSA Control Tower notifica os clientes quando ocorre um desvio, se os clientes desativarem o acesso confiável à AWS Control Tower em AWS Organizations. | 21 de setembro de 2023 |
| AWSControl Tower disponível em quatro unidades adicionais Regiões da AWS | Disponível na Ásia-Pacífico (Hyderabad), Europa (Espanha e Zurique) e Oriente Médio (). UAE | 13 de setembro de 2023 |
| AWSControl Tower disponível na região de Tel Aviv | AWSA Control Tower está disponível na região de Tel Aviv, il-central-1. | 28 de agosto de 2023 |
| AWSControl Tower lança 28 novos controles proativos | AWSA Control Tower lançou 28 novos controles proativos. | 24 de julho de 2023 |

| | | |
|---|---|---|
| AWSA Control Tower suspende o uso de 2 controles | AWSA Control Tower removerá dois controles da biblioteca de controles a partir de 18 de agosto de 2023. | 18 de julho de 2023 |
| AWSA zona de pouso 3.2 da Control Tower está disponível | AWSA versão 3.2 da zona de pouso do Control Tower está disponível. | 16 de junho de 2023 |
| AWSA Control Tower gerencia contas com base em ID | AWSA Control Tower rastreia o AWS ID da conta, em vez do endereço de e-mail da conta. | 14 de junho de 2023 |
| Controles de detetive adicionais do Security Hub disponíveis | AWSO Control Tower adiciona dez novos controles à bibliotec a de controles, para o Security Hub Service-Managed Standard: AWS Control Tower. | 12 de junho de 2023 |
| AWSA Control Tower publica tabelas de metadados de controle | AWSO Control Tower agora fornece tabelas de metadados de controle como parte da documentação publicada. | 7 de junho de 2023 |
| Suporte do Terraform para Account Factory Customiza tion | Suporte de região única para projetos de código aberto do Terraform em. AFC | 6 de junho de 2023 |
| AWS IAMautogestão disponível para landing zone | AWSA Control Tower agora ajuda os clientes a escolher seu provedor de identidade para um landing zone. | 6 de junho de 2023 |

| | | |
|---|---|---|
| Nova função adicionada | AWSA Control Tower adicionou uma nova função vinculada ao serviço e política associada. AWSServiceRoleForAWSControlTowerAWSControlTowerAccountServiceRolePolicy | 1.º de junho de 2023 |
| Atualização de governança mista | Atualização para aconselhar os clientes sobre governança mista. | 1.º de junho de 2023 |
| Controles proativos adicionais disponíveis | Novos controles proativos ajudam você a governar seu ambiente de várias contas e a atingir objetivos específicos de controle. | 19 de maio de 2023 |
| Sete regiões adicionais disponíveis | AWSO Control Tower agora está disponível em mais sete Regiões da AWS: Norte da Califórnia (São Francisco), Ásia-Pacífico (Hong Kong, Jacarta e Osaka), Europa (Milão), Oriente Médio (Bahrein) e África (Cidade do Cabo). | 19 de abril de 2023 |
| Mudança para uma política gerenciada | Alteramos o AWSControlTowerServiceRolePolicypara que o AWS Control Tower possa chamar os `EnableRegion` `ListRegions` ,, `GetRegionOptStatus` APIs que são implementados pelo AWS Serviço de gerenciamento de contas. | 6 de abril de 2023 |

| | | |
|---|---|---|
| Rastreamento de solicitações de personalização de conta geralmente disponível | AWSO Control Tower agora suporta a capacidade de rastrear solicitações de personalização de contas usando o fluxo de trabalho Account Factory for Terraform (AFT). | 16 de fevereiro de 2023 |
| IAMatualização de melhores práticas | Guia atualizado para se alinhar às recomendações de IAM melhores práticas. Para obter mais informações, consulte Melhores práticas de segurança em IAM. | 15 de fevereiro de 2023 |
| AWSDisponível na zona de pouso 3.1 da Control Tower | AWSA landing zone 3.1 da Control Tower está disponível. | 9 de fevereiro de 2023 |
| Controles proativos geralmente disponíveis | Os controles proativos são iniciados desde o status de pré-visualização até a disponibilidade geral. | 24 de janeiro de 2023 |
| Operações de conta simultânea | AWSO Control Tower agora suporta até cinco (5) ações simultâneas na fábrica de contas. Você pode criar, atualizar ou inscrever até cinco contas por vez. | 16 de dezembro de 2022 |
| Controles proativos auxiliam no provisionamento de recursos | AWSO Control Tower agora oferece suporte a controles proativos, implementados por meio de AWS CloudFormation ganchos. | 28 de novembro de 2022 |

| | | |
|---|---|---|
| Personalização de fábrica da conta disponível | AWSO Control Tower agora oferece suporte ao provision amento de contas com modelos de conta personali záveis, chamados de blueprint s, diretamente do console da Control TowerAWS. | 28 de novembro de 2022 |
| Status de conformidade visível para todos AWS Config regras | AWSO Control Tower agora exibe o status de conformid ade de todos AWS Config regras implantadas em unidades organizacionais registradas na AWS Control Tower. | 18 de novembro de 2022 |
| Mudança para uma política gerenciada | Alteramos o AWSContro lTowerServiceRolePolicypara que a AWS Control Tower possa assumir a `AWSContro lTowerBlueprintAcc ess` função, que é necessári a para as personalizações do Account Factory. | 28 de outubro de 2022 |
| APIspara controles, AWS CloudFormation recurso | AWSO Control Tower agora suporta ativação e desativaç ão de controles por meio de um conjunto de API chamadas e um novo AWS CloudForm ation recurso. | 1.º de setembro de 2022 |
| O cFct suporta a exclusão do conjunto de pilhas | O CFct suporta a exclusão de conjuntos de pilhas, definindo um parâmetro no arquivo de manifesto. | 26 de agosto de 2022 |

| | | |
|---|---|---|
| Retenção de registros personalizada | Você pode personalizar a política de retenção para buckets do Amazon S3 que armazenam seus CloudTrai l registros do AWS Control Tower, em incrementos de dias ou anos, até um máximo de 15 anos. | 15 de agosto de 2022 |
| Reparo de desvio de função disponível | AWSO Control Tower suporta o reparo do desvio de rolos, sem um reparo completo da landing zone. | 11 de agosto de 2022 |
| Versão 3.0 disponível | AWSA versão 3.0 da zona de pouso do Control Tower é alterada em relação à baseada em contas AWS CloudTrail trilhas para trilhas baseadas na organização e atualiza a política gerenciada para permitir trilhas em nível organizacional. Ele permite que você agregue AWS Config informações somente na sua região de origem. A versão 3.0 também inclui uma atualização para o controle de negação da região e dois novos controles de detetive. | 29 de julho de 2022 |
| A página Organização combina visualizações OUs e contas | A nova página Organização no AWS Control Tower mostra uma visão hierárquica de todas as unidades organizac ionais (OUs) e contas. | 18 de julho de 2022 |

| | | |
|---|---|---|
| Mudança para uma política gerenciada | Alteramos o AWSControlTowerServiceRolePolicypara que os clientes possam ter um nível organizacional AWS CloudTrail trilhas para agregar AWS CloudTrail troncos. | 20 de junho de 2022 |
| Inscrição e atualização mais fáceis para contas de membros | AWSO Control Tower agora oferece a capacidade de inscrever e atualizar contas de membros individualmente, de dentro da sua landing zone. Cada conta mostra quando está disponível para uma atualização. Separamos o botão Inscrever conta do fluxo de trabalho Criar conta no Account Factory. | 31 de maio de 2022 |
| AFTsuporta personalização para contas compartilhadas | AWSO Control Tower Account Factory for Terraform agora oferece suporte à personalização da conta de gerenciamento, arquivo de registros e contas de auditoria da AWS Control Tower. | 27 de maio de 2022 |
| Operações simultâneas para todos os controles opcionais | AWSO Control Tower agora permite que você aplique e remova proteções preventivas opcionais simultaneamente, bem como controles de detetive. | 18 de maio de 2022 |

| | | |
|---|---|---|
| Contas de segurança e registro existentes | AWSO Control Tower agora suporta a capacidade de trazer contas de segurança e registro existentes, em vez de criar novas durante a configuração da landing zone. | 16 de maio de 2022 |
| Versão 2.9 disponível | AWSA versão 2.9 da zona de pouso do Control Tower atualiza o encaminhador de notificações Lambda para usar o tempo de execução do Python versão 3.9. | 22 de abril de 2022 |
| Suporte atualizado para AWS melhores práticas, versão 2.8 disponível | AWSA versão 2.8 da zona de pouso da Control Tower fornece suporte adicional para garantir que suas cargas de trabalho e AWS as contas estão alinhadas com AWS melhores práticas. | 10 de fevereiro de 2022 |
| Região nega controle | AWSO Control Tower agora inclui um controle que ajuda você a restringir o acesso a AWS Regiões, para tratar de questões regulatórias e de conformidade. | 30 de novembro de 2021 |
| Controles de residência de dados | AWSO Control Tower agora oferece suporte a controles que ajudam você a gerenciar a residência de dados com controle granular. | 30 de novembro de 2021 |

| | | |
|---|---|---|
| AWSFábrica de contas Control Tower para Terraform | AWSO Control Tower agora oferece suporte ao Terraform para provisionamento e atualização automatizados de contas. | 29 de novembro de 2021 |
| Novo evento de ciclo de vida disponível | O `PrecheckOrganizationalUnit` evento registra se algum recurso impede o sucesso da tarefa de governança Extend, incluindo recursos aninhadosOUs. | 18 de novembro de 2021 |
| Aninhado disponível OUs | AWSO Control Tower agora permite que seu landing zone contenha estruturas de OU aninhadas. | 16 de novembro de 2021 |
| Detective: controle simultâneo | AWSOs controles de detetive da Control Tower agora oferecem suporte a operações simultâneas de ativação e desativação. | 5 de novembro de 2021 |
| Duas novas regiões disponíveis | AWSO Control Tower agora está disponível em dois novos AWS Regiões, região da Europa (Paris) e região da América do Sul (São Paulo). | 29 de julho de 2021 |
| Desseleção de região | Você pode desmarcar AWS Regiões que você não deseja mais governar por meio da AWS Control Tower. | 29 de julho de 2021 |

| | | |
|---|---|---|
| KMSchaves disponíveis | Opcionalmente, você pode criar ou escolher KMS as chaves que você gerencia para criptografar seus dados e recursos. | 28 de julho de 2021 |
| Mudança para uma política gerenciada | Alteramos o AWSContro lTowerServiceRolePolicypara que os clientes possam usar suas próprias chaves KMS de criptografia para AWS CloudTrail troncos. | 28 de julho de 2021 |
| Nomes de controle alterados, funcionalidade inalterada | Alguns nomes e descrições de controle foram atualizad os para refletir melhor as intenções políticas do controle, sem alteração na funcional idade. | 26 de julho de 2021 |
| Escaneamentos automatiz ados de arquivos gerenciados SCPs | AWSA Control Tower realiza escaneamentos automatiz ados diários do que foi gerenciado SCPs para verificar o desvio. | 11 de maio de 2021 |
| Nomes OUs e contas personalizados | AWSO Control Tower permite que você forneça nomes personalizados durante o processo de configuração da landing zone, para itens essenciais OUs e contas, sem criar desvios. | 16 de abril de 2021 |

| | | |
|---|---|---|
| Descomissionar uma landing zone é um autoatendimento | AWSO Control Tower agora permite que você desative uma landing zone sem entrar em contato AWS Support. O descomissionamento é um processo semiautomatizado que não pode ser desfeito. Não é o mesmo que excluir todos os recursos do AWS Control Tower manualmente. | 9 de abril de 2021 |
| Três regiões adicionais | AWSO Control Tower agora está disponível em mais três AWS Regiões: região Ásia-Pacífico (Tóquio), região Ásia-Pacífico (Seul) e região Ásia-Pacífico (Mumbai). | 8 de abril de 2021 |
| Novos controles do Log Archive, versão 2.7 da landing zone disponível | Quatro novos controles do Log Archive fornecem a governanç a do Log Archive sobre os recursos da AWS Control Tower, separadamente da governança dos recursos fora da AWS Control Tower. A orientação sobre quatro controles existentes mudou de obrigatória para eletiva. A versão 2.7 da landing zone do AWS Control Tower inclui um requisito paraHTTPS, que não pode ser desfeito após a atualização. | 8 de abril de 2021 |

| | | |
|---|---|---|
| Seleção de região | AWSA seleção da região da Control Tower oferece melhor capacidade de gerenciar a área geográfica dos recursos da AWS Control Tower. Para expandir o número de regiões nas quais você hospeda AWS recursos ou cargas de trabalho — por motivos de conformidade, regulamen tação, custo ou outros — agora você pode selecionar as regiões adicionais a serem governadas. | 19 de fevereiro de 2021 |
| Registre uma OU e controle todas as suas contas com a AWS Control Tower de uma só vez | AWSO Control Tower adiciona a capacidade de registrar uma OU, que é uma forma de colocar várias contas na governança ao mesmo tempo. | 28 de janeiro de 2021 |

| | | |
|---|---|---|
| Várias atualizações de conta estão registradas OUs | Agora você pode atualizar todas as contas em qualquer cadastrado AWS Organizat ions unidade organizacional (OU) contendo até 300 contas, com um único clique, no painel do AWS Control Tower. O recurso de atualização de várias contas, também conhecido como atualizaç ão em massa, elimina a necessidade de atualizar uma conta por vez ou de usar um script externo para realizar a atualização em várias contas juntas. | 28 de janeiro de 2021 |
| Nova função para agregar contas e contas não gerenciad as OUs | Uma nova função auxilia na detecção externa AWS Config regras, portanto, a AWS Control Tower não precisa obter acesso a contas não gerenciadas. | 29 de dezembro de 2020 |

| | | |
|---|---|---|
| AWSControl Tower está disponível em mais AWS Regiões. | AWSA Control Tower agora está disponível para ser implantada na região Ásia-Pacífico (Cingapura), Europa (Frankfurt), Europa (Londres), Europa (Estocolmo) e Canadá (Central). Com este lançamento, o AWS Control Tower está agora disponível em 10 AWS Regiões. Essa atualização da landing zone inclui todas as regiões listadas e não pode ser desfeita. Depois de atualizar sua landing zone para a versão 2.5, você deve atualizar manualmente todas as contas inscritas para que a AWS Control Tower governe nas 10 suportadas AWS Regiões. | 18 de novembro de 2020 |
| Atualização de controle | Uma versão atualizada foi lançada para o controle obrigatórioAWS-GR_IAM_ROLE_CHANGE_PROHIBITED . O controle atualizado permite o registro automatizado de contas com mais facilidade. | 8 de outubro de 2020 |
| A página de informações relacionadas agora está disponível para a AWS Control Tower | A página de informações relacionadas facilita a localização de tarefas comuns que podem ser úteis depois de configurar sua landing zone da AWS Control Tower. | 18 de setembro de 2020 |

| | | |
|---|---|---|
| AWSO console Control Tower mostra mais detalhes sobre contas OUs e contas. | No console do AWS Control Tower, você pode ver mais detalhes sobre seu AWS contas e unidades organizacionais (OUs). A página “Contas” agora lista todas as contas em sua organização, independentemente da OU ou do status de inscrição na AWS Control Tower. Agora você pode pesquisar, classificar e filtrar em todas as tabelas. | 22 de julho de 2020 |
| AWSO Control Tower permite que organizações existentes configurem uma landing zone | Agora você pode lançar uma landing zone para a AWS Control Tower em uma organização existente, para colocar a organização na governança. O recurso de provisionamento rápido de contas no AWS Control Tower foi renomeado para Enroll account e agora permite a inscrição de contas existentes AWS contas, bem como criação de novas contas. | 16 de abril de 2020 |

| | | |
|---|---|---|
| AWSA Control Tower agora está disponível na Ásia-Pacífico | AWSA Control Tower agora está disponível para ser implantada na Ásia-Pacífico (Sydney) AWS Região. Esta versão requer atualizações manuais nas contas vendidas, atualize somente se você planeja executar cargas de trabalho na Ásia-Pacífico (Sydney). | 3 de março de 2020 |
| É possível descomissionar uma zona de pouso da AWS Control Tower | AWS O Support pode ajudá-lo a descomissionar permanentemente uma landing zone por meio de um processo quase automatizado que preserva suas organizações, embora seja necessária alguma limpeza manual. | 27 de fevereiro de 2020 |
| O provisionamento rápido de contas está disponível no AWS Control Tower | O provisionamento rápido de contas facilita a execução de novas contas-membro quando a zona de destino está atualizada, com o recurso Enroll account (Registrar conta). | 20 de fevereiro de 2020 |
| Os eventos do ciclo de vida são monitorados na Control Tower AWS | Os eventos do ciclo de vida fornecem detalhes adicionais para determinados eventos da AWS Control Tower, para facilitar a automação do fluxo de trabalho. | 12 de dezembro de 2019 |

| | | |
|---|---|---|
| As páginas de configurações e atividades estão disponíveis para a AWS Control Tower | As páginas Settings (Configurações) e Activities (Atividades) facilitam a atualização da zona de destino e a visualização de eventos registrados em log. | 30 de novembro de 2019 |
| Controles preventivos adicionais estão disponíveis para a AWS Control Tower | Os controles preventivos no AWS Control Tower mantêm sua organização e seus recursos alinhados com seu ambiente. | 6 de setembro de 2019 |
| Controles de detetive adicionais estão disponíveis para a AWS Control Tower | Os controles de Detective na AWS Control Tower fornecem informações sobre o estado da sua organização e dos recursos. | 27 de agosto de 2019 |
| AWSA Control Tower agora está disponível ao público em geral | AWSO Control Tower é um serviço que oferece a maneira mais fácil de configurar e gerenciar sua conta múltipla AWS ambiente em grande escala. | 24 de junho de 2019 |

# AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário naGlossário da AWS Referência.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.