Guia do usuário

AWS Control Tower

AWS Control Tower: Guia 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 Organizations Para ajudar a evitar que suas organizações e contas apresentem desvio, o que é uma divergência das práticas recomendadas, o AWS Control Tower aplica controles (às vezes chamados de barreiras de proteção). Por exemplo, é possível usar controles para garantir que os logs de segurança e as permissões necessárias de acesso entre contas 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. É possível adotar o AWS Control Tower como sua principal forma de provisionar contas e infraestrutura. Com o AWS Control Tower, é possível aderir mais facilmente aos padrões corporativos, atender aos requisitos regulatórios e seguir as práticas recomendadas.

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, os administradores da nuvem central saberão que todas as contas estão alinhadas com 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

Atributos

O AWS Control Tower tem os seguintes recursos:

- Zona de pouso: uma zona de pouso é um ambiente de várias contas baseado nas práticas recomendadas 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, de detecção e proativos. Três categorias de orientação se aplicam aos controles: obrigatórias, altamente recomendadas ou eletivas. Para obter mais informações sobre controles, consulte Como os controles funcionam.
- Account Factory: um 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 obter mais informações, consulte Provisione e gerencie contas com o Account Factory.
- Painel: o painel oferece supervisão contínua da zona de pouso para a equipe de administradores da nuvem central. 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 obter 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 a inscrição de contas por meio de um Account Factory (ou “máquina de venda automática”), que é criada como uma abstração sobre os produtos provisionados no 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. Para obter mais informações sobre como criar e provisionar contas, consulte Métodos de provisionamento.

- 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, políticas de controle de serviços (SCPs) e políticas de controle de recursos (RCPs).

- 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. É possível 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 a 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. Consulte mais informações sobre como planejar e organizar a zona de pouso em Planejar a zona de pouso do AWS Control Tower e em AWS estratégia de várias contas para sua landing zone do AWS Control Tower.
2. Se você estiver pronto para criar a primeira zona de destino, consulte Conceitos básicos do AWS Control Tower.
3. Para obter informações sobre detecção e prevenção de oscilações, consulte Detectar e resolver desvios no AWS Control Tower.
4. Para obter detalhes de segurança, consulte Segurança no AWS Control Tower.
5. Consulte informações sobre como atualizar a zona de pouso e contas-membros em Gerenciamento de atualizações de configuração no AWS Control Tower.

Como o AWS Control Tower funciona

Esta seção descreve em nível geral 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 uma zona de pouso no AWS Control Tower é a seguinte:

- Root — O pai que contém todos os outros OUs em sua landing zone.
- UO de segurança: essa UO contém as contas de arquivamento de logs e de 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.
- UO de sandbox: a UO de sandbox é criada quando você inicia a zona de pouso, se você a habilita. Esse e outros registros OUs contêm as contas inscritas com as quais seus usuários trabalham para realizar suas AWS cargas de trabalho.
- Diretório do IAM Identity Center — Por padrão, esse diretório abriga os usuários do IAM Identity Center. Ele define o escopo de permissões para cada usuário do Centro de Identidade do IAM. Opcionalmente, você pode optar por autogerenciar sua identidade e controle de acesso. Para obter mais informações, consulte Como trabalhar com o AWS IAM Identity Center e o AWS Control Tower.
- 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 zona de pouso

Quando você configura uma zona de pouso, o AWS Control Tower realiza as seguintes ações na 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 UO de segurança: a conta de arquivamento de logs e a de auditoria.
- Cria um diretório nativo da nuvem no Centro de Identidade do IAM, com grupos pré-configurados e acesso de login único, se você escolher a configuração padrão do AWS Control Tower, ou permite que você autogerencie seu provedor de identidades.
- Aplica todos os controles obrigatórios e preventivos para implementar as políticas.

- Aplica todos os controles de detecção 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.

Gerenciar recursos com segurança dentro da zona de pouso e das 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 nem excluir esses recursos gerenciados pelo AWS Control Tower fora dos métodos compatíveis descritos neste guia. Excluir ou modificar esses recursos fará a zona de pouso entrar em um estado desconhecido. Para obter detalhes, consulte Orientações para criar e modificar recursos do 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.

O que são as contas compartilhadas?

No AWS Control Tower, três contas compartilhadas na zona de pouso são provisionadas durante a configuração: a conta de gerenciamento, a conta de arquivamento de logs e a conta de auditoria.

O que é a conta de gerenciamento?

É a conta que você criou especificamente para a zona de pouso. Essa conta é usada no faturamento de tudo na zona de pouso. Também é usado para provisionar contas no Account Factory, bem como para gerenciar OUs e controlar.

> **Note**
>
> Não é recomendado executar nenhum tipo de workload de produção em uma conta de gerenciamento do AWS Control Tower. Crie uma conta do AWS Control Tower separada para executar suas workloads.

Para obter mais informações, consulte Conta de gerenciamento.

O que é a conta de arquivamento de logs?

Essa conta funciona como um repositório para logs de atividades da API e configurações de recursos de todas as contas na zona de pouso.

Para obter 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 oferecer às equipes de segurança e conformidade o acesso de leitura e gravação a todas as contas na zona de pouso. 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. Consulte mais informações sobre perfis e funções do Lambda em Como configuro uma função do Lambda para assumir um perfil do IAM em outra conta da Conta da AWS?.

Para obter mais informações, consulte Conta de auditoria.

Como os controles funcionam

Um controle é uma regra de alto nível que fornece governança contínua para todo o ambiente da AWS . 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 da AWS Control Tower ou na AWS Control Tower APIs. Os controles obrigatórios são sempre aplicados e não podem ser alterados.

Os controles preventivos evitam que ações ocorram. Por exemplo, o controle eletivo chamado Não permitir alterações na política dos buckets do Amazon S3 (anteriormente chamado de Não permitir alterações na política de arquivamento de logs) impede qualquer alteração na política do IAM na conta compartilhada do arquivamento de logs. Qualquer tentativa de realizar uma ação impedida é negada e registrada no 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 Detect Whein Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances detecta se um volume não criptografado do Amazon EBS está conectado a EC2 uma instância 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 nas 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) e políticas de controle de recursos (RCPs). Os controles de detetive são implementados com AWS Config regras. Os controles proativos são implementados com AWS CloudFormation ganchos.

Related Topics

- Detectar e resolver desvios no AWS Control Tower

Como o AWS Control Tower funciona com StackSets

Por padrão, 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 breve resumo do comportamento esperado, com base nos parâmetros do AWS CloudFormation 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 análise de alguns termos que você encontra na documentação do 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 e OUs, consulte AWS Organizations terminologia e conceitos. Se você é iniciante no 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 O AWS 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 o Account Factory na AWS Control Tower. Às vezes, o Account Factory é chamado informalmente de “máquina de venda automática” de contas.
- Sua região de origem do AWS Control Tower é a AWS região na qual sua landing zone da AWS Control Tower foi implantada. Você pode ver sua região de origem nas configurações de zona inicial.
- O AWS Service Catalog permite gerenciar de forma central os serviços de TI comumente implantados. 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 dentro de 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 do AWS Control Tower. Para blogs técnicos que fornecem mais detalhes, consulte Related information.
- Uma linha de base no AWS Control Tower é um grupo de recursos e configurações específicas que você pode aplicar a um destino. O destino da linha de base mais comum pode ser uma unidade organizacional (UO). Por exemplo, a linha de base chamada `AWSControlTowerBaseline` está disponível para ajudar a registrar você 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.
- Esquema: um esquema é um artefato que encapsula alguns metadados, que descreve os componentes da infraestrutura implantados em uma conta. Por exemplo, um AWS CloudFormation modelo pode servir como um modelo para uma conta do AWS Control Tower.
- Desvio: uma alteração em um recurso instalado e configurado pelo AWS Control Tower. Recursos sem desvio permitem que o AWS Control Tower funcione adequadamente.
- 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 o AWS Control Tower cria automaticamente quando você configura a zona de pouso: a conta de gerenciamento, a conta de arquivamento de logs e a conta de auditoria. Você pode escolher nomes personalizados para a conta de arquivamento de logs e a conta de auditoria durante a configuração.
- Conta-membro: uma conta-membro pertence à organização do AWS Control Tower. A conta-membro pode ser inscrita ou não inscrita no AWS Control Tower. Quando uma UO registrada contém uma combinação de contas inscritas e não inscritas:
  - Os controles preventivos habilitados na UO 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. Consulte mais informações em Inheritance for service control policies na documentação do AWS Organizations .
  - Os controles de detecção habilitados na UO não se aplicam a contas não inscritas.

  Uma conta só pode ser membro de uma organização de cada vez e seus encargos são cobrados na conta de gerenciamento dessa organização. Uma conta-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 usuário do IAM) 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 ao AWS Control Tower por meio do processo de inscrição da conta ou registro da OU.
- Controle: um controle (também conhecido como barreira de proteção) é uma regra de alto nível que fornece governança contínua para o ambiente geral do AWS Control Tower. Cada controle impõe uma única regra. Os controles preventivos são implementados com SCPs. 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 pouso: uma zona de pouso é um ambiente em nuvem que oferece um ponto de partida recomendado, incluindo contas padrão, estrutura de contas, layouts de rede e segurança etc. Com uma zona de pouso, é possível implantar workloads que utilizam suas soluções e aplicações.
- UO aninhada: uma UO aninhada no AWS Control Tower é uma UO contida em outra UO. Uma UO pode ter exatamente uma UO principal e cada conta pode ser membro de exatamente uma UO. 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 UO aninhada no AWS Control Tower pode ter no máximo cinco níveis de profundidade.
- UO principal: a UO imediatamente acima da OU atual na hierarquia. Cada UO pode ter exatamente uma UO principal.
- OU secundária: qualquer UO abaixo da UO atual na hierarquia. Uma OU pode ter muitos filhos OUs.
- Hierarquia de OU: no AWS Control Tower, a hierarquia do aninhado OUs pode ter até cinco níveis. A ordem de aninhamento é chamada de Níveis. O topo da hierarquia é chamado de Nível 1.
- UO de nível superior: uma UO de nível superior é qualquer UO que esteja diretamente sob a raiz, não a raiz em si. A raiz não é considerada uma UO.
- Administrada: uma região administrada é gerenciada e controlada no ambiente pelo AWS Control Tower, de acordo com as políticas de governança definidas pela organização. Eles Regiões da AWS são monitorados de acordo com as melhores práticas e políticas organizacionais. Seus recursos nessas regiões são protegidos quando você habilita os controles do AWS Control Tower.
- Não administrada: regiões que mostram o status Não administrada não são controladas nem monitoradas pelo AWS Control Tower. Essas Regiões da AWS geralmente não aderem às

mesmas políticas de governança que o AWS Control Tower impõe. Você pode criar recursos nessas regiões, mas esses recursos não são protegidos pelos controles do AWS Control Tower.

- Negada: uma região negada é bloqueada especificamente pelo AWS Control Tower. Dentro do ambiente do AWS Control Tower, você não pode provisionar recursos nessas Regiões da AWS.

Preços

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. Consulte informações sobre os preços e as taxas associadas ao AWS Control Tower pricing.

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 Config Para obter detalhes, consulte Definição de preço do AWS 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, é possível 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 uma AWS conta e proteger sua conta AWS Control Tower de gerenciamento. Para obter informações sobre tarefas adicionais de configuração específicas para AWS Control Tower, consulteConceitos básicos do AWS Control Tower.

Inscreva-se para AWS

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

Anote o número AWS da sua conta, pois 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 um.

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-raiz tem acesso a todos os 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 AWS IAM Identity Center, habilite 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 AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

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

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

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

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

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

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

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

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

Segurança para contas

Você pode encontrar orientações adicionais sobre como configurar as melhores práticas que protegem a segurança de suas AWS Control Tower contas na AWS Organizations documentação.

- Best practices for the management account
- Best practices for member accounts

Próxima etapa

Conceitos básicos do AWS Control Tower

Conceitos básicos do 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 do AWS Control Tower ou APIs.

Se você é um AWS cliente atualmente, mas é novo no AWS Control Tower, talvez queira revisar a seção chamada Planejar a zona de pouso do 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. Caso prefira personalizar seu ambiente do AWS Control Tower imediatamente, consulte Etapa 2. Configure e inicie a zona de pouso .

> **Note**
>
> O AWS Control Tower configura serviços pagos AWS CloudTrail, como Amazon AWS Config CloudWatch, 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. Não é possível alterá-la depois de configurar a zona de pouso do AWS Control Tower. Consulte mais informações sobre como escolher uma região em Dicas administrativas para configuração da zona de pouso .

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

O procedimento de início rápido pressupõe que você aceitará os valores padrão para os recursos no ambiente do AWS Control Tower. Muitas dessas opções poderão ser alteradas mais tarde. Algumas opções únicas estão listadas na seção chamada Expectativas para a configuração da zona de pouso .

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 zona de pouso.
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 logs e uma conta de auditoria.
6. Confirme suas escolhas e selecione Configurar zona de pouso.
7. O AWS Control Tower leva cerca de 30 minutos para configurar todos os recursos na zona de pouso.

Para ter 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 iniciante e encontrar um problema de configuração, entre em contato com o AWS Support para solicitar assistência no diagnóstico.

Pré-requisito: verificações automáticas de pré-execução da conta de gerenciamento

Antes que o AWS Control Tower configure a zona de pouso, ele executa automaticamente uma série de verificações de pré-execução 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 alterações que estabelecem a zona de pouso. Aqui estão as verificações executadas pelo AWS Control Tower antes de configurar uma zona de pouso:

- Os limites de serviço existentes para o Conta da AWS devem ser suficientes para o lançamento do AWS Control Tower. Para obter mais informações, consulte Limitações e cotas no AWS Control Tower.
- Eles Conta da AWS devem ser assinantes dos seguintes AWS serviços:
  - Amazon Simple Storage Service (Amazon S3)
  - Nuvem de computação elástica da Amazon (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 Centro de Identidade do IAM só pode ser instalado na conta de gerenciamento de uma organização.
- Três opções se aplicam ao seu diretório do Centro de Identidade do IAM, com base na fonte de identidade que você escolher:
  - Repositório de Usuários do Centro de Identidade do IAM: se o AWS Control Tower estiver configurado com o Centro de Identidade do IAM, o AWS Control Tower cria grupos no diretório do Centro de Identidade do IAM e provisiona o acesso a esses grupos, para o usuário selecionado, para contas-membros.
  - Active Directory: se o Centro de Identidade do IAM para o AWS Control Tower estiver configurado com o Active Directory, o AWS Control Tower não gerenciará o diretório do Centro de Identidade do IAM. Ele não atribui usuários ou grupos a novas contas da AWS .
  - Provedor de identidade externo: se o Centro de Identidade do IAM para o AWS Control Tower estiver configurado com um provedor de identidades (IdP) externo, o AWS Control Tower criará grupos no diretório do Centro de Identidade do IAM e provisionará o acesso a esses grupos ao usuário selecionado para contas-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-fornecida ao sincronizar usuários com o mesmo nome entre o Centro de Identidade do IAM e o IdP externo. Você também pode criar grupos no 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 contas inscritas.

  Consulte mais informações sobre como trabalhar com o Centro de Identidade do IAM e o AWS Control Tower em O que você deve saber sobre as contas do Centro de Identidade do IAM 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. 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 zona de pouso. Para obter mais informações, consulte Inscrever contas que tenham recursos do AWS Config existentes.
- 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 o representante da sua conta da AWS para solicitar informações mais específicas de 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. Consulte informações sobre trilhas no nível da organização e o AWS Control Tower em Preços.

> **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.

Começar a usar o AWS Control Tower pelo console

Esse procedimento de introdução é destinado aos administradores do AWS Control Tower. Siga este procedimento quando estiver tudo pronto para configurar a zona de pouso usando o console do AWS Control Tower. Do início ao fim, ele 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 Planejar a zona de pouso do AWS Control Tower antes de continuar.

Tópicos

- Etapa 2. Configure e inicie a zona de pouso
- Etapa 3. Revisar e configurar a zona de pouso

Expectativas para a configuração da zona de pouso

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

Itens principais a serem definidos durante a configuração

- Você pode selecionar os nomes de UOs de nível superior durante a configuração e pode alterar os nomes de UOs depois de configurar a zona de pouso. 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 o AWS Control Tower cria, chamadas de arquivamento de logs 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 no 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 do landing zone, você pode escolher se deseja permitir que o AWS Control Tower configure uma AWS CloudTrail trilha em nível organizacional para sua organização, ou você pode optar por não usar trilhas gerenciadas pela AWS Control Tower e gerenciar suas próprias trilhas. CloudTrail Você pode optar por usar ou não as trilhas no nível organizacional que são gerenciadas pelo AWS Control Tower sempre que atualizar a zona de pouso.
- Se preferir, você poderá definir uma política de retenção personalizada para o bucket de log e o bucket de acesso ao log do Amazon S3 ao configurar ou atualizar a zona de pouso.
- Opcionalmente, você pode especificar um esquema previamente definido para usar no provisionamento de contas-membros personalizadas pelo console do AWS Control Tower. É possível personalizar as contas mais tarde caso você não tenha um esquema disponível. Consulte Personalizar contas com Account Factory Customization (AFC).

Opções de configuração que não podem ser desfeitas

- Não é possível alterar a região de origem depois que a zona de pouso é configurada.
- Se você estiver provisionando contas do Account Factory com, a VPCs VPC não CIDRs poderá ser alterada depois de criada.

Etapa 1: crie os endereços de e-mail de 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 exige 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 empresa que farão trabalhos específicos relacionados ao AWS Control Tower.
- Se você estiver configurando o AWS Control Tower pela primeira vez e se estiver trazendo contas existentes de segurança e arquivamento de log para o 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 de acesso às informações de auditoria disponibilizadas pelo 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 UO de segurança quando você cria a zona de pouso. Como prática recomendada, indicamos que, ao realizar ações nessas contas, seja utilizado um usuário do Centro de Identidade do IAM com as permissões com o escopo adequado.

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

para garantir que nenhum recurso esteja em conflito com os requisitos do AWS Control Tower. Se essas verificações não forem bem-sucedidas, a configuração da zona de pouso poderá 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 em log existentes.

Para fins de clareza, este Guia do usuário sempre se refere às contas compartilhadas por seus nomes padrão: de arquivamento de logs e de 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 as contas com os nomes personalizados na página Detalhes da conta.

Note

Estamos alterando nossa terminologia em relação aos nomes padrão de algumas unidades organizacionais do 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 UO de segurança era chamada de UO principal. A UO de sandbox era chamada de UO personalizada.

Etapa 2. Configure e inicie a zona de pouso

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

Important

Alterar sua região de origem depois de implantar sua zona de pouso do 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 a zona de pouso no console, execute a série de etapas a seguir.

Prepare-se: acesse o console do AWS Control Tower

1. Abra um navegador da web e navegue até o console do 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. Depois, escolha Configurar a zona de pouso.

Etapa 2a. Revise e selecione as regiões da AWS

Certifique-se de ter designado corretamente a AWS região que você selecionou para sua região de origem. Depois de implantar o AWS Control Tower, não é possível 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 pode 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 incorporar a governança do AWS Control Tower. A seleção da região de origem não é editável.

Como 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 habilitado.

Etapa 2b. Configure suas unidades organizacionais (OUs)

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

- UO fundamental: o AWS Control Tower depende de uma UO fundamental que é inicialmente chamada de UO de segurança. Você pode alterar o nome dessa UO durante a configuração

inicial e depois, na página de detalhes da UO. Essa UO de segurança contém as duas contas compartilhadas, que, por padrão, são chamadas de conta de arquivamento de logs e conta de auditoria.

- OU adicional — O AWS Control Tower pode configurar um ou mais adicionais OUs para você. Recomendamos que você provisione pelo menos uma UO adicional na zona de pouso, além da UO de segurança. Se essa UO adicional for destinada a projetos de desenvolvimento, recomendamos que você a nomeie como sandbox, conforme indicado em Diretrizes para configurar um ambiente bem arquitetado. Se você já tem uma OU existente em AWS Organizations, você pode ver a opção de pular a configuração de uma OU adicional no AWS Control Tower.

Etapa 2c. Configure as contas compartilhadas, o registro em log e a criptografia

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

Você deve fornecer endereços de e-mail exclusivos para as contas de arquivamento de logs e de auditoria e pode verificar o endereço de e-mail que forneceu anteriormente para a 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 do AWS Control Tower faz parte do nível raiz. A conta de gerenciamento permite o faturamento do AWS Control Tower. A conta também tem permissões de administrador para a zona de pouso. Você não pode criar contas separadas para faturamento e permissões de administrador no AWS Control Tower.

  O endereço de e-mail mostrado para a conta de gerenciamento não é editável durante essa fase de configuração. Ele 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 o 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 logs. 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.

Se desejar, configure a retenção de logs

Durante essa fase de configuração, você pode personalizar a política de retenção de logs para buckets do Amazon S3 que armazenam seus AWS CloudTrail registros no AWS Control Tower, em incrementos de dias ou anos, até um máximo de 15 anos. Se você optar por não personalizar sua retenção de logs, as configurações padrão são de um ano para registro em log de conta padrão e 10 anos para registro em log de acesso. Esse recurso também está disponível quando você atualiza ou redefine a zona de pouso.

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 AWS do IAM Identity Center que você pode configurar e personalizar por conta própria, ou com outro método, como um IdP externo, seja para federação direta de contas ou federação de várias contas por meio do IAM Identity Center. É possível alterar essa seleção posteriormente.

Por padrão, o AWS Control Tower configura o AWS IAM Identity Center para sua landing zone, de acordo com a orientação de melhores práticas definida 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 permitida. Essa opção se aplica somente à zona de pouso como um todo.

Para obter mais informações, consulte Orientações sobre o Centro de Identidade do IAM.

Opcionalmente, configure trilhas AWS CloudTrail

Como prática recomendada, sugerimos que você configure o registro em log. Se você quiser permitir que o 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 aceitar ou recusar trilhas do nível da organização ao atualizar a zona de pouso.

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.

Se desejar, configure AWS KMS keys

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

Quando você seleciona Configurar zona de pouso, o AWS Control Tower realiza uma pré-verificação para validar sua chave do KMS. A chave também deve atender a estes requisitos:

- Habilitada
- Simétrica
- Não ser uma chave multirregional
- Ter as permissões corretas adicionadas à política
- Estar na conta de gerenciamento

Poderá ser exibido um banner de erro se a chave não atender a esses requisitos. Nesse caso, escolha outra chave ou gere uma. Certifique-se de atualizar a política de permissões da chave, conforme descrito na próxima seção.

Atualizar a política de chave do KMS

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

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

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

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

Como atualizar a política de chave do KMS

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 chave, verifique se você consegue visualizar a política de chave. Se você não conseguir visualizar a política de chave, escolha Alternar para a visualização da política.
5. Escolha Editar e atualize a política de chaves padrão do KMS adicionando as seguintes declarações de política para AWS Config e. CloudTrail

   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 chave do KMS

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

```
{
    "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 seguintes páginas:

- Granting encrypt permissions no Guia do usuário do AWS CloudTrail .
- Required Permissions for the KMS Key When Using Service-Linked RolesS3 Bucket Delivery) no Guia do desenvolvedor do AWS Config .

> **Proteção contra invasores**
>
> Ao adicionar determinadas condições às suas políticas, você pode ajudar a evitar um tipo específico de ataque, conhecido como ataque confused deputy, que ocorre se uma entidade coagir uma entidade com mais privilégios a realizar uma ação, como a falsificação de identidade entre serviços. Também consulte informações gerais sobre condições de política em Especificar condições em uma política.

O AWS Key Management Service (AWS KMS) permite que você crie chaves KMS multirregionais e chaves assimétricas; no entanto, o AWS Control Tower não oferece suporte a chaves multirregionais ou chaves assimétricas. O AWS Control Tower realiza uma pré-verificação das chaves existentes. Você poderá receber uma mensagem de erro se selecionar uma chave multirregional ou uma chave assimétrica. Nesse caso, gere outra chave para usar com os recursos do 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-membros personalizadas

Ao seguir o fluxo de trabalho Criar conta para adicionar suas contas-membros, você pode, opcionalmente, especificar um esquema previamente definido para usar no provisionamento de contas-membros personalizadas pelo console do AWS Control Tower. É possível personalizar as contas mais tarde caso você não tenha um esquema disponível. Consulte Personalizar contas com Account Factory Customization (AFC).

Etapa 3. Revisar e configurar a zona de pouso

A próxima seção da configuração mostra as permissões que o AWS Control Tower exige para a zona de pouso. 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.

Como finalizar

1. No console, revise as permissões do serviço e, quando estiver pronto, escolha Eu entendo as permissões que o 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 zona de pouso.

Essa série de etapas inicia o processo de configuração da zona de pouso, 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 assinaturas do SNS

O endereço de e-mail fornecido para a conta de auditoria receberá e-mails de Notificação da AWS : confirmação da assinatura de cada região da AWS compatível com o 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 pelo AWS Control Tower.

Comece a usar o AWS Control Tower usando APIs

Esse procedimento de introdução é destinado aos administradores do 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 do AWS Control Tower de forma programática, seja por meio do AWS CloudFormation console ou do AWS CLI.

Antes de iniciar a zona de pouso do AWS Control Tower, realize estas tarefas de pré-requisito:

- Determine a região de origem mais apropriada. Para obter mais informações, consulte Dicas administrativas para configuração da zona de pouso .

- Consulte Pré-requisito: verificações automáticas de pré-execução da 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 a zona de pouso.

Tópicos

Expectativas para a configuração da landing zone com APIs

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

Itens principais a serem definidos durante a configuração

- Você pode selecionar os nomes das UOs fundamentais durante a configuração e pode alterar os nomes das UOs depois de configurar a zona de pouso. 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 o AWS Control Tower cria, chamadas de arquivamento de logs e auditoria por padrão, mas não pode alterar esses nomes após a configuração. (Essa é uma seleção única.)
- Durante a configuração com APIs, você deve especificar AWS 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 cadastrá-las no 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 do landing zone, você pode escolher se deseja permitir que o AWS Control Tower configure uma AWS CloudTrail trilha em nível organizacional para sua organização, ou você pode optar por não usar trilhas gerenciadas pela AWS Control Tower e gerenciar suas próprias trilhas. CloudTrail Você pode optar por usar ou não as trilhas no nível organizacional que são gerenciadas pelo AWS Control Tower sempre que atualizar a zona de pouso.
- Se preferir, você poderá definir uma política de retenção personalizada para o bucket de log e o bucket de acesso ao log do Amazon S3 ao configurar ou atualizar a zona de pouso.

Opções de configuração que não podem ser desfeitas

- Não é possível alterar a região de origem depois que a zona de pouso é configurada.
- Se você estiver provisionando contas com, a VPCs VPC não CIDRs poderá ser alterada depois que elas forem criadas.

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

Etapa 1: configure a zona de pouso

O processo de configuração da zona de pouso do AWS Control Tower tem várias etapas. Certos aspectos da 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 iniciar a zona de pouso, consulte Expectativas para a configuração da zona de pouso .

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

- criando uma nova AWS Organizations organização,
- configurar os endereços de e-mail da conta compartilhada;
- e criar uma função do IAM ou um usuário do IAM Identity Center com as permissões necessárias para chamar a landing zone APIs.

Etapa 1. Crie a organização que conterá a zona de pouso:

1. Chame a AWS Organizations `CreateOrganization` API e ative todos os recursos para criar a OU básica. Inicialmente, o AWS Control Tower a chama de UO de segurança. Essa UO de segurança contém as duas contas compartilhadas, que, por padrão, são chamadas de conta de arquivamento de logs e conta de auditoria.

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

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

Etapa 2. Provisione contas compartilhadas, se necessário:

Para configurar a zona de pouso, o AWS Control Tower exige 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 empresa que farão trabalhos específicos relacionados ao 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. Chame a AWS Organizations `CreateAccount` API 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 a AWS Organizations `DescribeAccount` API.

Etapa 3. Crie os perfis de serviço necessários

Crie as seguintes funções de serviço do IAM no caminho `/service-role/` do IAM que permitem que o AWS Control Tower realize as chamadas de API necessárias para configurar sua landing zone:

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

Consulte mais informações sobre essas políticas e suas permissões em Uso de políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower.

Como criar um perfil do IAM:

1. Crie uma função do IAM com as permissões necessárias para chamar toda a landing zone APIs. Como alternativa, você pode criar um usuário do Centro de Identidade do IAM e atribuir as permissões necessárias.

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

```
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess",
                "organizations:DeregisterDelegatedAdministrator"
                "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 a zona de pouso

A `CreateLandingZone` API do AWS Control Tower exige uma versão da zona de pouso e um arquivo de manifesto da zona de destino como parâmetros de entrada. Você pode usar o arquivo de manifesto da zona de pouso do AWS Control Tower para configurar os seguintes recursos:

- Se desejar, configure a retenção de logs
- Opcionalmente, Conta da AWS autogerencie o acesso
- Opcionalmente, configure trilhas AWS CloudTrail
- Se desejar, configure AWS KMS keys

Após compilar seu arquivo de manifesto, estará tudo pronto para criar uma zona de pouso.

Para obter mais informações sobre o que está no arquivo de manifesto, consulte Exibir os detalhes do arquivo de manifesto do seu landing zone.

Para obter mais informações sobre os esquemas da zona de pouso que se aplicam ao arquivo de manifesto da zona de pouso, consulte Esquemas da zona de pouso.

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

1. Chame a API `CreateLandingZone` do AWS Control Tower. Essa API requer uma versão da zona de pouso e um arquivo de manifesto da zona de destino como entrada.

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

   Para obter mais detalhes sobre o conteúdo do arquivo de manifesto do landing zone, consulteVeja os detalhes do arquivo de manifesto do seu landing zone.

   O exemplo a seguir mostra um LandingZoneManifestmanifesto.json, que inclui configurações para regiões governadas e registro centralizado:

   ```
   {
      "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.

O exemplo a seguir mostra um arquivo de LandingZoneManifestmanifesto.json, que inclui configurações para backup e registro centralizado:

```
{
        "landingZoneIdentifier": "LANDING ZONE ARN",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "backup": {
                "configurations": {
                    "centralBackup": {
                        "accountId": "CENTRAL BACKUP ACCOUNT ID"
                    },
```

```
                    "backupAdmin": {
                        "accountId": "BACKUP MANAGER ACCOUNT ID"
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
                },
                "enabled": true
            },
            "governedRegions": [
                "us-west-1"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 365
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 3650
                    }
                },
                "enabled": true
            }
        },
        "version": "3.3"
}
```

Saída:

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

2. Chame a API `GetLandingZoneOperation` para conferir o status da operação `CreateLandingZone`. A API `GetLandingZoneOperation` 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 poderá chamar a API `GetLandingZone` para revisar a configuração da zona de pouso.

```
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 a zona de pouso

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

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

Para regiões opcionais, a API `ListLandingZones` só retornará o identificador da zona de pouso se você chamar a API na mesma região da região de origem da API. Por exemplo, se a zona de pouso estiver configurada em af-south-1 e você chamar `ListLandingZones` em af-south-1, a API retornará o identificador da zona de pouso. Se a zona de pouso estiver configurada em af-south-1 e você chamar `ListLandingZonesem` ap-east-1, a API não retornará o identificador da zona de pouso.

Saída:

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

Atualizar a zona de pouso

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 a `UpdateLandingZone` API e fazer referência a um arquivo de manifesto atualizado da zona de pouso. Essa API retorna um `0perationIdentifier`, que você pode usar ao chamar a API `GetLandingZone0peration` para verificar o status da operação de atualização.

Como atualizar a zona de pouso

1. Ligue para a `UpdateLandingZone` API do AWS Control Tower e consulte a versão atualizada da zona de destino ou o arquivo de manifesto atualizado da zona de destino.

   ```
   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
   ```

Exemplo de LandingZoneManifest arquivo.json, com regiões e registro centralizado:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
```

```
            "name": "Security"
        },
        "sandbox": {
            "name": "Sandbox"
        }
    },
    "centralizedLogging": {
         "accountId": "LOG ARCHIVE ACCOUNT ID",
         "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": "SECURITY ACCOUNT ID"
    },
    "accessManagement": {
         "enabled": true
    }
}
```

Saída:

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

Opcionalmente, registre novamente a UO para atualizar as contas

Para a AWS Control Tower registrada OUs com menos de 1.000 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.

Redefinir a zona de pouso 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 organização usam a zona de pouso, podem ocorrer alterações no status de conformidade. Essas mudanças são chamadas de desvio.

Para identificar se a zona de pouso está com desvio, você pode chamar a API `GetLandingZone`. Essa API retorna o status de desvio da zona de pouso de `DRIFTED` ou`IN_SYNC`.

Para resolver o desvio na zona de pouso, você pode usar a API `ResetLandingZone` para redefinir a zona de pouso à configuração original. Por exemplo, o AWS Control Tower habilita 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 poderá usar a API `ResetLandingZone` se tiver a versão mais recente disponível da zona de pouso. É possível chamar a API `GetLandingZone` e comparar a versão da sua zona de pouso com a versão mais recente disponível. Se necessário, você pode Atualizar a zona de pouso para que a zona de pouso use a versão mais recente disponível. Nesses exemplos, estamos usando a versão 3.3 como a mais recente.

1. Chame a API `GetLandingZone`. Se a API retornar um status de desvio de `DRIFTED`, a zona de pouso estará com desvio.
2. Chame a API `ResetLandingZone` para redefinir a zona de pouso 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 detalhes sobre a atualização da versão da zona de pouso em Atualizar a zona de pouso .

Veja os detalhes do arquivo de manifesto do seu landing zone

O arquivo de manifesto da zona de pouso do AWS Control Tower é um arquivo de texto que descreve seus recursos da AWS Control Tower. As seções a seguir mostram definições detalhadas das entradas no arquivo de manifesto do landing zone.

Para ver um exemplo completo do esquema da zona de pouso, consulte Esquemas da zona de pouso.

Regiões governadas — Regiões a serem colocadas sob governança

- Tipo: lista de strings
- Obrigatório: não
- Exemplo:

```
"governedRegions": ["us-west-2","us-west-1"]
```

Estrutura da organização — Selecione os nomes de segurança e sandbox OUs a serem criados em sua organização

- Tipo: Objeto
- Obrigatório: Sim
- Propriedades:
- Exemplo:
  - `security`- um objeto com uma propriedade necessárianame, que assume um `String`
  - `sandbox`- um objeto com uma propriedade necessárianame, que assume um `String`

```
"organizationStructure": {
       "security": {
           "name": "CORE"
```

```
        },
        "sandbox": {
            "name": "Sandbox"
        }
    }
```

Registro centralizado — Configuração para AWS CloudTrail

- Tipo: Objeto
- Obrigatório: Sim
- Propriedades:
  - accountId - a) representa `String` a conta na qual AWS o recurso de registro deve ser implantado
  - configurações - e `Object` com três propriedades
    - `loggingBucket`- um objeto com uma propriedade`retentionDays`, que assume um `Number`
    - `accessLoggingBucket`- um objeto com uma propriedade`retentionDays`, que assume um `Number`
    - `kmsKeyArn`- um opcional `String`
  - ativado - um opcional `Boolean`
- Exemplo:

```
"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 — Escolha onde implantar o recurso de registro

- Tipo: Objeto
- Obrigatório: Sim
- Properties: accountId - `String` uma que representa AWS a conta na qual o recurso de registro deve ser implantado
- Exemplo:

```
"securityRoles": {
        "accountId": "333333333333"
   }
```

Gerenciamento de acesso — escolha se deseja ativar o gerenciamento de acesso

- Tipo: Objeto
- Obrigatório: não
- Propriedades: ativado - um booleano
- Exemplo:

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

backup — Configuração para AWS backup com o AWS Control Tower

- Tipo: Objeto
- Obrigatório: não
- Propriedades:
  - configurações - e `Object` com três propriedades
    - `centralBackup`- um objeto com uma propriedade`accountId`, que assume um `String`
    - `backupAdmin`- um objeto com uma propriedade`accountId`, que assume um `String`
    - `kmsKeyArn`- um opcional `String`
  - ativado - um `Boolean`
- Exemplo:

```
"backup": {
    "configurations": {
        "centralBackup": {
            "accountId": "CENTRAL BACKUP ACCOUNT ID"
        },
        "backupAdmin": {
            "accountId": "BACKUP MANAGER ACCOUNT ID"
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-
ecfXXXXXXXXX"
    },
    "enabled": true
}
```

Visualizar o status das operações da zona de pouso

A API `ListLandingZoneOperations` permite que você visualize o status das operações do AWS Control Tower que realizam ações na zona de pouso.

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

ListLandingZoneOperations

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

Esse 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"
        }
    ]
}
```

Esse 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 com APIs apenas

Este demonstração de exemplos é um documento complementar. Para obter explicações, ressalvas e mais informações, consulte Como começar a usar o AWS Control Tower usando. APIs

Pré-requisitos

Antes de criar uma zona de pouso do AWS Control Tower, você deve criar uma organização, duas contas compartilhadas e alguns perfis do IAM. Este tutorial de demonstração 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 o perfil do IAM necessário.

`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 a conta IDs e gere o arquivo de manifesto do landing zone.

Os dois primeiros comandos no exemplo a seguir armazenam a conta IDs das contas que você criou na Etapa 1 em variáveis. Essas variáveis então ajudam a gerar o arquivo de manifesto da zona de pouso.

```
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 zona de pouso com a versão mais recente.

Você deve configurar a zona de pouso 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 zona de pouso configurando um loop.

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

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

Exemplo de saída do status:

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

Você pode usar o script de exemplo a seguir para ajudar a configurar um loop, que relata o status da operação repetidamente, como um arquivo de log. Então você não precisa continuar inserindo 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
```

Como mostrar informações detalhadas sobre a zona de pouso

Etapa 1. Encontre o ARN da zona de pouso

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

A saída incluirá o identificador da zona de pouso, como mostrado no exemplo de resultado 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
```

Veja a seguir 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 API do **`ListLandingZoneOperations`** para ver o status de qualquer operação que mude a zona de pouso.

Para rastrear o status de qualquer operação da zona de pouso, você pode chamar a API ListLandingZoneOperations.

Esquemas da zona de pouso

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 3.1 e mais recentes, são publicados nesta seção de referência para ajudar você a escolher uma versão compatível.

> **Note**
>
> Um problema conhecido relacionado ao registro em log de acesso desnecessário está presente na zona de pouso versão 3.0. O problema foi resolvido na zona de pouso versão 3.1. Consulte mais informações sobre essas alterações em Versão 3.1 da zona de pouso do AWS Control Tower.

Esquema da zona de pouso 3.1

```
{
    "type": "object",
```

```
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "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
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
```

```
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "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
        },
        "OrganizationalUnit": {
            "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/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "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": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "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
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
```

```
            "required": [
                "configurations"
            ]
        }
    },
    "BackupAdminConfigurations": {
        "type": "object",
        "required": [
            "accountId"
        ],
        "properties": {
            "accountId": {
                "type": "string",
                "maxLength": 12,
                "minLength": 12,
                "pattern": "^\\d{12}$",
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "BackupConfigurations": {
        "type": "object",
        "required": [
            "backupAdmin",
            "centralBackup",
            "kmsKeyArn"
        ],
        "properties": {
            "backupAdmin": {
                "$ref": "#/definitions/BackupAdminConfigurations"
            },
            "centralBackup": {
                "$ref": "#/definitions/CentralBackupConfigurations"
            },
            "kmsKeyArn": {
                "type": "string",
                "maxLength": 2048,
                "minLength": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
```

```
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "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
        },
        "OrganizationalUnit": {
            "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/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "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"
```

```
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$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
        },
        "Backup": {
            "type": "object",
            "properties": {
```

```
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
```

```
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "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
        },
        "OrganizationalUnit": {
            "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": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "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
        }
    }
}
```

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 a AWS Organizations `CreateOrganization` API para criar uma organização e ativar todos os recursos.

   Consulte instruções mais detalhadas em Etapa 1: configure a zona de pouso .
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 de arquivamento de log (às vezes chamada de conta de “Registro em log”)
   - Conta de auditoria (às vezes chamada de conta “Segurança”)
   - As funções AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations, e AWSControlTowerStackSetRolede serviço.

     Consulte informações sobre como o AWS Control Tower usa esses perfis para realizar chamadas de API da zona de pouso em Etapa 1: configurar a 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: Array
    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 desvios em uma landing zone, você pode usar o console do AWS Control Tower AWS CLI, o ou a `ResetLandingZone`API.

Próximas etapas

Agora que a zona de pouso 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.
- É possível configurar usuários e grupos do Centro de Identidade do IAM com perfis e permissões específicos. Para obter recomendações, consulte Recomendações para configurar grupos, perfis 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 obter mais informações, consulte Permissões para configurar e provisionar contas.
- Para garantir Validação de conformidade do AWS Control Tower, os administradores da nuvem central podem revisar os arquivos de log na conta de arquivamento de logs, e os auditores de terceiros designados podem revisar as informações de auditoria na conta de auditoria (compartilhada), que é membro da UO de segurança.
- Para saber mais sobre os recursos do AWS Control Tower, consulte Related information.
- 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 obter mais informações, consulte Gerenciamento de atualizações de configuração no AWS Control Tower.
- Se você enfrentar problemas ao usar o AWS Control Tower consulte Solução de problemas.

> **Important**
>
> Se você ainda não ativou a MFA para o usuário-raiz da conta, faça isso agora. Consulte mais informações sobre as práticas recomendadas para o usuário-raiz em As práticas recomendadas do usuário raiz para o Conta da AWS.

Limitações e cotas no 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 a zona de pouso devido a um problema de cota de serviço, entre em contato com o AWS Support.

Consulte mais informações sobre limitações específicas de controles em Limitações de controle.

> **Guia de referência de controles**
>
> Informações detalhadas sobre os controles do AWS Control Tower foram transferidas para o Guia de referência de controles do AWS Control Tower.

Limitações conhecidas no AWS Control Tower

Esta seção descreve limitações conhecidas e casos de uso incompatíveis no AWS Control Tower.

- O AWS Control Tower tem limitações gerais de simultaneidade. Em geral, é permitida uma operação por vez. 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 uma API.
  - 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 cancelamento do gerenciamento de contas deve ser realizado em uma conta por vez.
- Os endereços de e-mail das contas compartilhadas na UO de segurança podem ser alterados, mas você deve atualizar a zona de pouso para ver essas alterações no console do AWS Control Tower.
- Um limite de cinco (5) SCPs por OU se aplica à OUs sua landing zone do AWS Control Tower.
- O AWS Control Tower suporta até 10.000 contas na organização da sua zona de destino, divididas entre todas as suas OUs.
- 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 registro OUs, consulteLimitações com base nos serviços da AWS subjacentes.

- As personalizações do AWS Control Tower (cFct) não estão disponíveis nestes Regiões da AWS, porque algumas dependências não estão disponíveis:
  - Região Europa (Zurique), eu-central-2
  - Região Europa (Espanha), eu-south-2
  - Oeste do Canadá (Calgary)
  - AWS Região Ásia-Pacífico (Malásia), ap-southeast-5

  Será possível implantar e gerenciar recursos nessas regiões com o CfCT, se você implantar o CfCT na sua região de origem do AWS Control Tower, mas não poderá criar o CfCT nessas regiões.
- O AWS Control Tower Account Factory for Terraform (AFT) não está disponível no seguinte Regiões da AWS, porque algumas dependências não estão disponíveis:
  - Região Europa (Zurique), eu-central-2
  - Região Europa (Espanha), eu-south-2
  - Oeste do Canadá (Calgary)
  - AWS Região Ásia-Pacífico (Malásia), ap-southeast-5
- O AWS Control Tower Account Factory for Terraform (AFT) não pode ser implantado por novos clientes do AFT nas seguintes regiões, porque o AWS CodeStar Connections não está disponível para conexão com um sistema de controle de versão (VCS) de terceiros:
  - Ásia-Pacífico (Hong Kong), África (Cidade do Cabo), Oriente Médio (Bahrein), Europa (Zurique), Ásia-Pacífico (Jacarta), Ásia-Pacífico (Hyderabad), Asia Pacific (Osaka), Ásia-Pacífico (Melbourne), Israel (Tel Aviv), Europa (Espanha) e Oriente Médio (EAU)
- As regiões a seguir não são compatíveis com o Centro de Identidade do IAM.
  - AWS Região Ásia-Pacífico (Malásia), ap-southeast-5

  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 regiões a seguir não são compatíveis com o AWS Service Catalog.
  - Oeste do Canadá (Calgary) ca-west-1
  - AWS Região Ásia-Pacífico (Malásia), ap-southeast-5

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

- Ao chamar uma API de controle para ativar ou desativar um controle, o limite de atualizações de `EnableControl` e `DisableControl` no AWS Control Tower é de 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.
- Ao provisionar contas por meio do Account Factory Customizations (AFC), com esquemas baseados no Terraform, você pode implantar esses esquemas em apenas uma Região da AWS. Por padrão, o AWS Control Tower é implantado na região de origem.

Solicitar um aumento da cota

O console do Service Quotas fornece informações sobre as cotas do 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 simultâneas: o número máximo de operações de conta simultâneas que podem ser executadas ao mesmo tempo. Padrão: 5, máximo: 10, ajustável
- Número de contas em uma única UO: o número máximo de contas gerenciadas do AWS Control Tower que podem estar presentes em uma UO. Se você adicionar contas além desse limite, o processo de registro da UO no AWS Control Tower não poderá ser executado. Para saber mais sobre o número de contas por UO, consulte Limitações com base nos serviços da AWS subjacentes na documentação do 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 do AWS Control Tower podem mudar após o aumento da cota. Por exemplo, pode levar mais tempo para atualizar uma UO quando você tem mais contas nela. Ou pode levar mais tempo para concluir uma ação em uma OU com cinco SCPs do que com três SCPs.

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

Como alternativa, você pode entrar em contato com o AWS Support para solicitar um aumento de cota para alguns recursos no AWS Control Tower. Ou você pode assistir ao vídeo a seguir e aprender como automatizar determinados aumentos da cota de serviço.

Vídeo: Automatizar solicitações para aumentos de cota de serviço em serviços relacionados ao AWS Control Tower

Este vídeo (7:24) descreve como automatizar o aumento da cota de AWS serviços relacionados e integrados, com base em implantações no AWS Control Tower. 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.

Vídeo de demonstração de aumentos de cotas no AWS Control Tower.

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

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

Limitações de controle

O AWS 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 serviços (SCPs), AWS Config regras e AWS CloudFormation ganchos.

> **Guia de referência de controles**
>
> Informações detalhadas sobre os controles do AWS Control Tower foram transferidas para o Guia de referência de controles do AWS Control Tower.

Se você modificar os recursos da AWS Control Tower, como um SCP, ou remover qualquer AWS Config recurso, como um gravador ou agregador do Config, a AWS Control Tower 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**
>
> O AWS 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, ao implanta esse controle, ele pode não operar em todas as regiões que você administra com o AWS Control Tower. Essa limitação afeta certos controles de detecção, certos controles proativos e certos controles no padrão gerenciado por serviço do Security Hub: AWS Control Tower. Consulte mais informações sobre a disponibilidade regional em Security Hub controls. Consulte também a documentação da lista de serviços regionais e a documentação de referência de controles do Security Hub.

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

Consulte mais informações sobre como o AWS Control Tower gerencia as limitações de regiões e controles em Considerações sobre como ativar as regiões opcionais da AWS.

> **Note**
>
> Para ter as informações mais atualizadas sobre controles e suporte de região, recomendamos que você chame as operações de API `GetControl` e `ListControls`.

Encontrar controles e regiões disponíveis

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

Consulte também a tabela de referência dos controles do AWS Control Tower e das regiões compatíveis em Control availability by Region no Guia de referência de controles do AWS Control Tower.

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

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

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

A tabela a seguir mostra os controles de detecção do AWS Control Tower que não são compatíveis com algumas Regiões da AWS.

Identificador de controle	Regiões não implantáveis
`API_GW_CACHE_ENABLED_AND_ENCRYPTED`	ap-sudeste-5, ca-west-1
`APPSYNC_ASSOCIATED_WITH_WAF`	af-south-1, ap-south-2, ap-sudeste-3, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-sul-2, il-central-2, il-central-2, il-central-2, il-central-2 1, me-central-1

Identificador de controle	Regiões não implantáveis
AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, eu-sul-2, il-central-1, me-central-1, me-central-1 me-central-1
AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, eu-sul-2, il-central-1, me-central-1, me-central-1 me-central-1
AUTOSCALING_CAPACITY_REBALANCING	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, eu-sul-2, il-central-1, me-central-1, me-central-1 me-central-1
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-nordeste-3, ap-sudeste-3, ap-sudeste-3, ap-sudeste-4, ap-sudeste-5, ca-west-1, il-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1, ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ap-west-1, eu-central-2, eu-sul-1, eu-central-2, eu-sul-1, eu-south-1, eu-south-1 eu-south-2, il-central-1, me-central-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ap-sudeste-5, 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	ap-sudeste-5, ca-west-1

Identificador de controle	Regiões não implantáveis
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-sudeste-5, ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-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, ap-southeast-5, ca-west-1, eu-central-2, ap-southeast-2, eu-sul-1, eu-sul-2, il-central-1, me-central-1
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_IAM_USER_MFA_ENABLED	ap-south-2, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, me-central-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	ap-south-2, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-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-southeast-5, ca-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-south-1, eu-south-2, il-central-1
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2

Identificador de controle	Regiões não implantáveis
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, ap-southeast-5, ca-west-1, eu-south-2
AWS-GR_RESTRICTED_SSH	af-south-1, eu-south-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	ap-sudeste-5, ca-oest-1, il-central-1, me-central-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	eu-central-2, eu-south-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, ap-southeast-5, ca-west-1, eu-central-2, ap-southeast-2, eu-sul-1, eu-sul-2, il-central-1, me-central-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	ap-sudeste-5, ca-west-1, il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, eu-sul-2, il-central-1, me-central-1, me-central-1 me-central-1
BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, eu-sul-2, il-central-1, me-central-1, me-central-1 me-central-1

Identificador de controle	Regiões não implantáveis
BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK	ap-south-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ca-west-1, eu-central-2, eu-south-2, eu-south-2, il-central-1, eu-sul-2, il-central-1, me-central-1, me-central-1 me-central-1

Limitações com base nos serviços da AWS subjacentes

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

Diretrizes gerais

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

- Com 15 regiões governadas, OUs há suporte para até 1000 contas.
- Com 16 a 21 regiões administradas, o tamanho máximo de UO permitido está na faixa de 600 a 1.000 contas.
- Com 22 regiões governadas, há OUs suporte para até 680 contas.
- Com 23 ou mais regiões administradas, o tamanho máximo de OU suportado é inferior a 680 contas.

Em caso de erro

Se o registro falhar, você poderá tentar Registrar novamente a UO. Além disso, é possível diminuir a UO usando uma UO aninhada ou transferindo contas para outra UO.

> **Note**
>
> Os controles obrigatórios que o AWS Control Tower sempre impõe não são contabilizados no número de controles que você habilitou em uma UO, 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 UO. Por exemplo, se 15 regiões forem governadas e 15 controles opcionais estiverem habilitados, o limite para registrar a UO será de mil 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 são contabilizadas nesse limite: é possível inscrever até mil novas contas no AWS Control Tower a cada semana.

Limitações iniciais para contas e regiões opcionais

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 UO devido à latência.

Diferenças regionais para a 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 Customization (AFC) não está disponível porque o Service Catalog não está disponível para oferecer suporte à funcionalidade subjacente dos esquemas.
- 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 determinar melhor o comportamento do ambiente do AWS Control Tower, verifique sua região de origem. Depois, avalie os itens a seguir. Consulte mais detalhes em Limitations and quotas in AWS Control Tower.

- Está AWS Service Catalog disponível na região de origem desejada?
- Os controles de que você precisa estão disponíveis? Consulte Control limitations.
- O Centro de Identidade do IAM está disponível na região de origem desejada?

Regiões implantáveis para controles

O AWS Control Tower não pode ativar determinados controles quando você os implanta em determinadas regiões, devido à falta de dependências subjacentes. Você pode encontrar as informações mais atualizadas sobre as regiões implantáveis para qualquer controle chamando `ListControls` e. `GetControl` APIs Você também pode ver as regiões implantáveis no console do AWS Control Tower.

Quando você ativa um controle em uma OU que é governada pela AWS Control Tower, a área efetiva do controle é a interseção das suas regiões governadas pela AWS Control Tower com as regiões implantáveis do controle.

Por exemplo, um controle pode ser ativado em uma OU que opera nas Regiões X, Y e Z governadas. Mas depois de ativado, o mesmo controle é implantado somente nas Regiões X e Z, porque o controle em si não oferece suporte à Região Y.

É importante monitorar as relações entre os controles que você implanta e as regiões em que você opera cargas de trabalho no AWS Control Tower, para que você não tenha lacunas na proteção de seus AWS recursos.

Como verificar suas regiões protegidas

- No console do AWS Control Tower, você pode ver os controles e regiões habilitados na seção Controles habilitados.
- Se você chamar a `GetEnabledControl` API, o parâmetro TargetRegions mostrará somente as regiões nas quais você pode implantar o controle de forma eficaz, não as regiões não implantáveis.

Guia de referência do AWS Control Tower Controls

Informações detalhadas sobre os controles no AWS Control Tower foram transferidas para o Guia de referência de controles do AWS Control Tower.

Práticas recomendadas para administradores do AWS Control Tower

Este tópico destina-se principalmente a administradores da conta de gerenciamento.

Os administradores da conta de gerenciamento são responsáveis por explicar algumas tarefas que os controles do AWS Control Tower impedem que os administradores de contas-membros executem. Este tópico descreve algumas práticas recomendadas e procedimentos para transferir esse conhecimento e fornece outras dicas para configurar e fazer a manutenção do ambiente do AWS Control Tower de forma eficiente.

Explicar o acesso aos usuários

O console do AWS Control Tower está disponível somente para usuários com as permissões de administrador da conta de gerenciamento. Somente esses usuários podem executar o trabalho administrativo na zona de pouso. De acordo com as práticas recomendadas, isso significa que a maioria dos seus usuários e administradores de contas-membros nunca verá o console do AWS Control Tower. Como membro do grupo de administradores da conta de gerenciamento, é sua responsabilidade explicar as informações a seguir aos usuários e administradores de suas contas-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.

Explicar o acesso a 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 entidade do IAM, 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.
- Simulador de políticas do IAM: com ele, é possível testar e solucionar problemas em políticas baseadas no IAM e em recursos. Consulte mais informações, consulte Testar políticas do IAM com o simulador de políticas do IAM.
- 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 realizadas pelos administradores da zona de pouso do AWS Control Tower podem ser vistas na conta de gerenciamento da zona de pouso. As ações realizadas pelos administradores de contas-membros e usuários podem ser vistas na conta de arquivamento de logs compartilhada.

  É possível visualizar uma tabela de resumo de eventos do AWS Control Tower na página Atividades.

Explicar os controles preventivos

Um controle preventivo garante que as contas de sua organização mantenham a conformidade com as políticas corporativas. O status de um controle preventivo é aplicado ou não habilitado. Um controle preventivo evita violações de políticas usando políticas de controle de serviço (SCPs). Em comparação, um controle de detecção informa você sobre vários eventos ou estados que existem, por meio de regras definidas do 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.

Como mostrar os controles preventivos para usuários que precisam dessa informação

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 UO e os controles que se aplicam a ela.
5. Repita as duas etapas anteriores para cada UO sobre a qual o usuário precisa de informações.

Consulte informações detalhadas sobre os controles e suas funções em About controls in AWS Control Tower.

Planejar a zona de pouso do AWS Control Tower

Quando você passa pelo processo de configuração, o AWS Control Tower inicia um recurso principal associado à sua conta, chamado zona de pouso, que serve como uma casa para suas organizações e suas contas.

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

Consulte informações sobre algumas das práticas recomendadas a serem seguidas ao planejar e configurar a zona de pouso em AWS estratégia de várias contas para sua landing zone do AWS Control Tower.

Maneiras de configurar o AWS Control Tower

É possível configurar uma zona de pouso do AWS Control Tower em uma organização existente ou começar criando uma organização que contenha sua zona de pouso do AWS Control Tower.

- Iniciar o AWS Control Tower em uma organização existente: Esta seção é para clientes que já AWS Organizations estão prontos para serem adotados pela AWS Control Tower.
- Iniciar o 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 do AWS Control Tower da zona de pouso existente para algumas ou todas as suas contas existentes OUs e dentro de uma organização. Consulte Govern existing organizations and accounts.

Comparar funcionalidades

Aqui está uma breve comparação das diferenças entre adicionar o AWS Control Tower a uma organização existente ou estender a governança do AWS Control Tower para contas OUs e contas. Além disso, algumas considerações especiais se aplicam se você estiver migrando da solução AWS Landing Zone para o 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 Console da AWS . Nesse caso, você já tem uma organização que você criou 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, o 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 no AWS Control Tower, o que significa que já existe uma landing zone para essa organização. Estender a governança significa que os controles do 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 está 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. O AWS Control Tower não pode realizar pré-verificações para determinar se o AWS Control Tower pode interferir na implantação atual da zona de pouso. Para obter mais informações, consulte Demonstração: mude do ALZ para o AWS Control Tower. Além disso, consulte informações sobre como mover contas de uma zona de pouso para outra em Se a conta não atender aos pré-requisitos

Iniciar o AWS Control Tower em uma organização existente

Ao configurar uma landing zone do AWS Control Tower em uma organização existente, você pode começar a trabalhar imediatamente, paralelamente ao seu AWS Organizations ambiente atual. 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.

O AWS Control Tower consolida usando a conta de gerenciamento da organização existente como sua conta de gerenciamento. Nenhuma nova conta de gerenciamento é necessária. É possível iniciar sua zona de pouso do AWS Control Tower por 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 do AWS Control Tower à sua organização existente

O AWS Control Tower adiciona duas contas à sua organização: uma conta de auditoria e uma conta de registro em log. Essas contas mantêm um registro das ações realizadas por sua equipe, em suas contas de usuário final individuais. As contas de Auditoria e Arquivamento de logs aparecem na UO de Segurança na zona de pouso do AWS Control Tower.

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

Resumo dos recursos

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

- Ele permite a cobrança unificada em todos os grupos da organização, pois as contas adicionadas pelo AWS Control Tower farão parte da sua organização existente.
- Ele permite administrar todas as contas de uma conta de gerenciamento em sua UO.
- Ele simplifica a forma como você aplica os controles que abrangem a segurança e a conformidade para 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 executar o AWS Control Tower em sua organização existente, siga o processo descrito em Conceitos básicos do AWS Control Tower.

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

Iniciar o AWS Control Tower em uma nova organização

Se você é novo no AWS Control Tower e ainda não trabalhou com ele AWS Organizations, o melhor lugar para começar é com nosso Configuração documento.

O AWS Control Tower configura uma organização automaticamente quando você não tem uma configurada.

AWS estratégia de várias contas para sua landing zone do AWS Control Tower

Os clientes do AWS 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 do 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 a zona de pouso for configurada, o AWS Control Tower continuará ajudando você a manter suas políticas corporativas e práticas de segurança em várias contas e workloads.

A maioria das zonas de pouso se desenvolve com o tempo. À medida que o número de unidades organizacionais (OUs) e contas na sua 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. Esse capítulo fornece orientações prescritivas sobre como planejar e configurar a zona de pouso do AWS Control Tower, de acordo com a estratégia de várias contas da AWS , 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 nas contas da AWS como contêineres de recursos isolados: elas oferecem categorização da workload, bem como redução do raio de alcance 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 da 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 workload.

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.

O AWS 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.

O AWS Control Tower oferece uma zona de pouso que é configurada automaticamente. Ele impõe controles para garantir a conformidade com suas diretrizes corporativas em várias contas em seu ambiente.

Definição de um zona de pouso

> A zona de pouso é um ambiente de nuvem que oferece um ponto de partida recomendado, incluindo contas padrão, estrutura de contas, layouts de rede e segurança e assim por diante. Com uma zona de pouso, é possível implantar workloads que utilizam suas soluções e aplicações.

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

Usar várias contas da AWS

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

- Controle de segurança: as aplicações têm diferentes perfis de segurança, portanto exigem políticas e mecanismos de controle diferentes. Por exemplo, é mais fácil falar com um auditor e apontar para uma única conta que hospeda a workload do setor de cartões de pagamento (PCI).
- Isolamento: uma conta é uma unidade de proteção de segurança. Os possíveis riscos e as ameaças à segurança devem estar contidos em uma conta sem afetar outras. Portanto, as necessidades de segurança podem exigir que você isole as contas umas das outras. Por exemplo, é possível 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 sobre a Proteção de Dados (GDPR).
- Processo empresarial: as unidades de negócios ou produtos costumam ter finalidades e processos completamente diferentes. Contas individuais podem ser estabelecidas para atender às necessidades específicas do negócio.
- Faturamento: uma conta é a única maneira verdadeira de separar itens em um nível de faturamento, incluindo coisas como taxas de transferência e assim por diante. A estratégia de várias contas ajuda a criar itens separados passíveis de cobrança em unidades de negócios, equipes funcionais ou usuários individuais.
- Alocação de cotas — as AWS cotas são configuradas por conta. A separação das workloads em contas diferentes dá a cada conta (como um projeto) uma cota individual bem definida.

Usar várias unidades organizacionais

O AWS Control Tower e outras estruturas de orquestração de contas podem fazer alterações que ultrapassam os limites da conta. Portanto, as AWS melhores práticas abordam 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, de produção e de preparação.

Além disso, AWS as contas geralmente são agrupadas em unidades organizacionais (OUs), para fins de governança e controle. OUs são 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 ambiente de produção, com controles e políticas distintos. Os ambientes de produção e preparação podem ser criados e administrados separadamente e faturados como contas separadas OUs. Além disso, você pode querer configurar uma UO de sandbox para testes de código.

Use uma estrutura bem planejada para OUs sua landing zone

O AWS Control Tower configura alguns OUs para você automaticamente. À medida que suas workloads e seus requisitos se expandem com o tempo, você pode estender a configuração original da zona de pouso 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 o AWS Control Tower configurar a primeira OU necessária para você — a OU de segurança —, recomendamos criar outras OUs na sua landing zone.

Recomendamos que você permita que o AWS Control Tower crie pelo menos uma UO adicional, chamada UO de sandbox. Essa UO é para seus ambientes de desenvolvimento de software. O AWS

Control Tower pode configurar a UO de sandbox para você durante a criação da zona de pouso, caso a selecione.

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 do AWS Control Tower na página de unidades organizacionais.

Recomendado, OUs além dos configurados automaticamente

- UO de infraestrutura: contém seus serviços compartilhados e contas de rede.

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

- UO de sandbox: uma UO de desenvolvimento de software. Por exemplo, ela pode ter um limite fixo de gastos ou pode não estar conectada à rede de produção.

> **Note**
>
> O AWS Control Tower recomenda que você configure a UO de sandbox, mas ela é opcional. Ela pode ser configurada automaticamente como parte da configuração da zona de pouso.

- UO de workloads: contém contas que executam suas workloads.

> **Note**
>
> O AWS Control Tower não configura a UO de workloads para você.

Consulte mais informações em Production starter organization with AWS Control Tower.

Exemplo do AWS Control Tower com uma estrutura completa de UO de várias contas

O AWS Control Tower permite definir uma hierarquia de UO 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 do AWS Control Tower de acordo com a orientação estratégica de AWS várias contas.

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

- Para ver um diagrama que mostra um conjunto de exemplos OUs em um ambiente expandido e plano do AWS Control Tower com orientação para AWS várias contas, consulte Exemplo: cargas de trabalho em uma estrutura de OU plana.
- Consulte mais informações sobre como o AWS Control Tower funciona com estruturas de UO aninhada em Aninhado OUs na AWS Control Tower.
- Para obter mais informações sobre como o 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:

- UO Security_Prod: fornece uma área somente leitura para políticas de segurança, bem como uma área de auditoria de segurança emergencial.
- UO de infraestrutura — Talvez você queira separar a OU de infraestrutura, recomendada anteriormente, em duas OUs, 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 duas OUs, 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 a raiz

A raiz não é uma UO. É um contêiner para a conta de gerenciamento e para todas as OUs contas da sua organização. Conceitualmente, a raiz contém todos os. OUs Ela não pode ser excluída. Não é possível administrar contas inscritas no nível de raiz no 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 zona de pouso

Aqui estão algumas dicas para configurar sua zona de pouso.

- A AWS região onde você trabalha mais deve ser sua região de origem.
- Configure a zona de pouso e implante as contas do Account Factory de dentro de sua região de origem.
- 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 AWS Control Tower. Recomendamos que você não mova esses buckets.
- É possível criar seus próprios buckets de log na conta de arquivamento de logs, mas não é recomendado. Certifique-se de deixar os buckets criados pelo AWS Control Tower.
- Seus logs de acesso ao Amazon S3 devem estar na mesma AWS região dos buckets de origem.
- Durante o lançamento, 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.
- AWS Control Tower permite a marcação apenas de controles habilitados. Para obter mais informações, consulte AWS Control Tower permite a marcação de controles habilitados.

- Recomendamos habilitar a autenticação multifator (MFA) para cada conta gerenciada pelo AWS Control Tower.
- Como alternativa, você pode usar o recurso de gerenciamento de acesso AWS raiz, que permite que ações raiz sejam executadas nas contas dos membros e elimina a necessidade de ativar o MFA para cada conta. Para obter mais informações, consulte Gerenciamento centralizado do acesso root para clientes que usam AWS Organizations.

Considerações sobre VPCs

- A VPC criada pela AWS Control Tower é limitada àquela Regiões da AWS em que a AWS Control Tower está disponível. Alguns clientes com workloads que são executadas em regiões incompatíveis podem querer desabilitar a VPC criada com a conta do Account Factory. Eles podem preferir criar uma VPC usando o portfólio do Service Catalog ou criar uma VPC personalizada que seja executada somente nas regiões necessárias.
- A VPC criada pelo AWS Control Tower não é a mesma que a VPC padrão criada para todas as Contas da AWS. Nas regiões compatíveis com o AWS Control Tower, o AWS Control Tower exclui a VPC padrão ao criar a VPC do AWS Control Tower.
- Se você excluir sua VPC padrão em sua AWS região de origem, é melhor excluí-la em todas as outras AWS regiões.

Recomendações para configurar grupos, perfis 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 ser acessível somente à equipe de segurança, a conta de gerenciamento deve ser acessível somente à equipe de administradores da nuvem, e assim por diante.

Consulte mais informações sobre esse tópico em Gerenciamento de identidade e acesso no AWS Control Tower.

Restrições recomendadas

Você pode restringir o escopo do acesso administrativo às suas organizações configurando um perfil ou uma política do IAM que permita que os administradores gerenciem somente ações do AWS Control Tower. A abordagem recomendada é usar a política do IAM `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`. Com o perfil `AWSControlTowerServiceRolePolicy` habilitado, 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 do perfil para restringir as contas e os recursos que interagem com determinados perfis no AWS Control Tower. É altamente recomendável que você restrinja o acesso ao perfil `AWSControlTowerAdmin`, pois ele permite amplas permissões de acesso. Consulte mais informações em Optional conditions for your role trust relationships.

Orientações para criar e modificar recursos do AWS Control Tower

Indicamos a seguir as práticas recomendadas para criar e modificar recursos no AWS Control Tower. Essas orientações podem mudar à medida que o serviço é atualizado. Lembre-se de que o modelo de responsabilidade compartilhada se aplica ao seu ambiente do AWS Control Tower.

Orientação geral

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

  Em particular:

  - Mantenha um AWS Config gravador ativo. Se você excluir o gravador do Config, os controles de detecção 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 de segurança (OU). A modificação dessas funções pode exigir uma atualização da sua zona de destino.
  - Não exclua o perfil `AWSControlTowerExecution` de suas contas-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 capacidade de negar a região da torre de controle da AWS, conforme mostrado no controle, negue 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 outro. SCPs A alteração nessa SCP não é relatada como um desvio. No entanto, algumas mudanças poderão afetar a funcionalidade do AWS Control Tower de maneiras imprevisíveis, se o acesso a determinados recursos for negado. Por exemplo, se o SCP for desanexado ou modificado, uma conta poderá perder o acesso a um AWS Config gravador ou criar uma lacuna no registro. CloudTrail
- Não use a 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, certos recursos de detecção de desvios do AWS Control Tower poderão não funcionar adequadamente sem o suporte de mensagens do AWS Organizations. Esses recursos de detecção de desvios ajudam a garantir que o AWS Control Tower possa relatar o status de conformidade de unidades organizacionais, contas e controles em sua organização com precisão. Para obter mais informações, consulte .API_DisableAWSServiceAccess na Referência da AWS Organizations API.
- Em geral, o AWS Control Tower executa uma única ação por vez, que deve ser concluída para que a outra ação possa começar. Por exemplo, se você tentar provisionar uma conta enquanto o processo de habilitação de um controle já estiver em operação, ocorrerá uma falha no provisionamento de contas.

  Exceção:

  - O AWS Control Tower permite ações simultâneas para implantar controles opcionais. Consulte mais informações em Concurrent deployment for optional controls.
  - O AWS Control Tower permite até dez ações simultâneas de criação, atualização ou inscrição em contas com o Account Factory.

> **Note**
>
> Consulte mais informações sobre os recursos criados pelo AWS Control Tower em O que são as contas compartilhadas?.

Dicas sobre contas e OUs

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

Quando fazer login como usuário-raiz

Determinadas tarefas administrativas exigem que você faça login como usuário raiz. Você pode fazer login como usuário root em um Conta da AWS que foi criado pela fábrica de contas no 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.

- Consulte mais informações sobre as ações que exigem credenciais de login de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia de referência do AWS Gerenciamento de contas .

> **Note**
>
> Para alterar ou habilitar seu plano do AWS Support, você precisa fazer login como usuário-raiz ou ser um usuário com as permissões apropriadas do IAM.

Para fazer login como usuário raiz

1. Abra a página de login da AWS .

   Se você não tiver o endereço de e-mail Conta da AWS ao qual precisa de acesso, você pode obtê-lo no 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 login da AWS e faça login com a senha redefinida.

Como alternativa, você pode usar o AWS recurso de Gerenciamento de Acesso Raiz, que permite que ações raiz sejam executadas nas contas dos membros, sem precisar fazer login como Root. Para obter mais informações, consulte Gerenciamento centralizado do acesso root para clientes que usam AWS Organizations.

AWS Organizations orientação

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

- Você pode encontrar orientações sobre as melhores práticas para proteger a segurança da sua conta de gerenciamento do AWS Control Tower e das contas dos membros na AWS Organizations documentação.
  - Best practices for the management account
  - Best practices for member accounts
- Não atualize as políticas de controle de serviço existentes (SCPs) anexadas a uma OU registrada no AWS Control Tower. Isso pode fazer com que os controles entrem em um estado desconhecido, o que exigirá que você redefina a zona de pouso ou registre novamente sua UO no AWS Control Tower. Em vez disso, você pode usar AWS Organizations para criar novos SCPs e anexá-los ao que o AWS Control Tower criou em OUs vez de editar. SCPs
- Mover contas individuais, já inscritas, para o AWS Control Tower, de fora de uma UO registrada, causa um desvio que deve ser resolvido. Consulte Tipos de deriva 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 for necessário acessar essas contas por meio de SSO, consulte Acesso à conta-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.
- O AWS Control Tower lida com a filtragem de permissões de forma diferente do que AWS Organizations faz. Se suas contas forem provisionadas com a fábrica de contas do AWS Control Tower, os usuários finais poderão ver os nomes e os pais de todas OUs no console do AWS Control Tower, mesmo que não tenham permissão para recuperar esses nomes e pais diretamente. AWS Organizations
- O AWS Control Tower não é compatível com permissões mistas em organizações, como permissão para visualizar a UO principal de uma UO, mas não para ver os nomes de UO. Por esse motivo, espera-se que os administradores do AWS Control Tower tenham permissões completas.
- O AWS Organizations `FullAWSAccess` SCP deve ser aplicado e não deve ser mesclado com outro. SCPs A alteração nessa SCP não é relatada como um desvio. No entanto, algumas mudanças poderão afetar a funcionalidade do AWS Control Tower de maneiras imprevisíveis, se o acesso a determinados recursos for negado. Por exemplo, se o SCP for desanexado ou modificado, uma conta poderá perder o acesso a um AWS Config gravador ou criar uma lacuna no registro. CloudTrail
- Não use a 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, certos recursos de detecção de desvios do AWS Control Tower poderão não funcionar adequadamente sem o suporte de mensagens do AWS Organizations. Esses recursos de detecção de desvios ajudam a garantir que o AWS Control Tower possa relatar o status de conformidade de unidades organizacionais, contas e controles em sua organização com precisão. Para obter mais informações, consulte .API_DisableAWSServiceAccess na Referência da AWS Organizations API.

Orientações sobre o Centro de Identidade do IAM

O AWS 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 Centro de Identidade do IAM para você, se você configura o Centro de Identidade do IAM por conta própria, de uma forma que atenda às suas necessidades de negócios com mais eficiência ou se deseja selecionar outro método para acessar a conta.

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

Por padrão, o AWS Control Tower configura o AWS IAM Identity Center para sua landing zone, de acordo com a orientação de melhores práticas definida 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.

Escolher uma opção

No console, você pode optar por autogerenciar o Centro de Identidade do IAM durante o processo de configuração da zona de pouso, em vez de permitir que o AWS Control Tower o configure para você. A qualquer momento, você pode optar por alterar essa seleção, modificando as configurações de zona inicial e atualizando-a na página Configurações de zona inicial.

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

1. Acesse a página Configurações de zona inicial.
2. Selecione a guia Configurações.
3. Em seguida, escolha o botão de opção apropriado para alterar sua seleção para o AWS IAM Identity Center.

Depois de escolher autogerenciar o AWS IAM Identity Center como seu IdP, o AWS Control Tower cria somente as funções e políticas necessárias para gerenciar a AWS Control Tower, como e. `AWSControlTowerAdmin` `AWSControlTowerAdminPolicy` Para zonas de pouso que se autogerenciam, o AWS Control Tower não cria mais perfis e agrupamentos do IAM 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 do AWS Control Tower, os usuários, grupos e conjuntos de permissões criados pelo 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 AWS do 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 perfis a qualquer momento, modificando as configurações de zona inicial.

- Para obter informações específicas sobre como o AWS Control Tower funciona com o IAM Identity Center com base na sua fonte de identidade, consulte Considerações para AWS IAM Identity Center clientes na seção Verificações de pré-lançamento da página de conceitos básicos deste Guia do usuário.
- Consulte mais informações sobre como o comportamento do AWS Control Tower interage com o Centro de Identidade do IAM e diferentes fontes de identidades em Considerations for Changing Your Identity Source no Guia do usuário do Centro de Identidade do IAM.
- Consulte mais informações sobre como trabalhar com o AWS Control Tower e o Centro de Identidade do IAM em Trabalhando com o AWS IAM Identity Center e o AWS Control Tower.

Orientações sobre o Account Factory

Você pode encontrar problemas ao usar o Account Factory para provisionar uma nova conta no AWS Control Tower. Consulte informações sobre como solucionar esses problemas na seção Falha no provisionamento de novas contas em Troubleshooting no Guia do usuário do AWS Control Tower.

Recomendamos que você crie usuários federados ou perfis do IAM em vez de usuários do IAM. Usuários federados e perfis do IAM fornecem credenciais temporárias. Os usuários do IAM têm credenciais de longo prazo que podem ser difíceis de gerenciar. Consulte mais informações em Identidades do IAM (usuários, grupos de usuários e perfis) no Guia do usuário do IAM.

Se você estiver autenticado como usuário do IAM ou do IAM Identity Center ao provisionar uma nova conta no Account Factory ou ao usar o recurso de inscrição da conta AWS Control Tower, verifique se o usuário tem acesso ao seu portfólio. AWS Service Catalog Caso contrário, você poderá receber uma mensagem de erro do Service Catalog. Consulte mais informações em Nenhum erro de caminhos de inicialização encontrado na seção Troubleshooting no Guia do usuário do AWS Control Tower.

> **Note**
>
> É possível provisionar até cinco contas por vez.

Orientações sobre como assinar os tópicos do SNS

Assine tópicos do SNS para ter informações sobre seu ambiente do AWS Control Tower.

- O tópico do `aws-controltower-AllConfigNotifications` SNS recebe todos os eventos publicados pela AWS Config, incluindo notificações de conformidade e notificações de CloudWatch eventos da Amazon. Por exemplo, esse tópico informa se ocorreu uma violação de controle. Ele também fornece informações sobre outros tipos de eventos. (Saiba mais sobre o AWS Config, referente a o que é publicado quando esse tópico é configurado.)
- Eventos de dados da trilha `aws-controltower-BaselineCloudTrail` também estão configurados para serem publicados no tópico `aws-controltower-AllConfigNotifications` do SNS.
- Para receber notificações de conformidade detalhadas, recomendamos que você assine o tópico `aws-controltower-AllConfigNotifications` do SNS. Esse tópico agrega notificações de conformidade de todas as contas secundárias.

- Para receber notificações de desvios e outras, bem como de conformidade, mas menos notificações em geral, recomendamos que você assine o tópico `aws-controltower-AggregateSecurityNotifications` do SNS.
- Para receber notificações sobre erros do AWS Control Tower Account Factory for Terraform (AFT), você pode se inscrever em um tópico do SNS chamado aft_failure_notifications, exibido no repositório AFT. Por exemplo:

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

- Todos os tópicos do SNS são criptografados em repouso com criptografia de disco. Consulte mais informações em Data encryption.

Consulte mais informações sobre tópicos e conformidade do SNS em Prevention and notification.

Orientações sobre chaves do KMS

O AWS Control Tower funciona com AWS Key Management Service (AWS KMS). Opcionalmente, se quiser criptografar e descriptografar seus recursos do AWS Control Tower com uma chave de criptografia gerenciada por você, será possível gerar e configurar AWS KMS keys. Você pode adicionar ou alterar uma chave do KMS sempre que atualizar a zona de pouso. Como uma prática recomendada, é aconselhável usar suas próprias chaves do KMS e alterá-las de tempos em tempos.

AWS KMS permite criar chaves KMS multirregionais e chaves assimétricas. No entanto, o AWS Control Tower não é compatível com chaves multirregionais ou chaves assimétricas. O AWS Control Tower realiza uma pré-verificação das chaves existentes. Você poderá receber uma mensagem de erro se selecionar uma chave multirregional ou uma chave assimétrica. Nesse caso, gere outra chave para usar com os recursos do AWS Control Tower.

Para clientes que operam um cluster AWS CloudHSM: Crie um armazenamento de chaves personalizado associado ao seu cluster CloudHSM. Depois, é possível criar uma chave do KMS, que reside no armazenamento de chaves personalizado do CloudHSM que você criou. É possível adicionar essa chave do KMS ao AWS Control Tower.

Você deve fazer uma atualização específica na política de permissões de uma chave do KMS para que ela funcione com o AWS Control Tower. Consulte mais detalhes na seção chamada Atualizar a política de chave do KMS.

Práticas recomendadas para atualizações de zona de pouso

Esta seção apresenta algumas considerações e práticas recomendadas que você deve ter em mente ao considerar uma atualização da versão de zona de pouso no AWS Control Tower. A mudança da série da versão 2.0 da zona de pouso para a série da versão 3.0 da zona de pouso é especialmente importante. Ao atualizar a zona de pouso, 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 zona de pouso.

Resumo das práticas recomendadas explicadas nesta seção

- Prática recomendada: por motivos de segurança e auditoria, é altamente recomendável que você habilite o registro em log geral, para todas as contas, e envie as informações do registro em log para um local centralizado. No AWS Control Tower, esse local centralizado é a conta de arquivamento Log, que fornece um bucket de registro do Amazon S3.
- Melhor prática: se você optar por não participar da CloudTrail trilha em nível organizacional no AWS Control Tower, configure e gerencie suas próprias trilhas.
- Prática recomendada: ao operar o ambiente do 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 logs
- Controles obrigatórios aprimorados
- Maior número de controles disponíveis

- Integrado com AWS Security Hub
- Atualizações de runtime do Python

Precauções ao 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 oferece mais suporte a AWS CloudTrail trilhas gerenciadas em nível de conta. AWS
- Você tem a opção de escolher uma trilha em nível organizacional gerenciada pelo 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 UO não estiverem inscritas no AWS Control Tower e tiverem suas próprias trilhas no nível de conta que você deseja manter.

Considerações sobre a escolha de trilhas em nível organizacional CloudTrail

- Ao fazer upgrade para a versão 3.0 ou posterior, o AWS Control Tower exclui as trilhas no nível da conta que ele criou originalmente, após 24 horas. [Exceção]
- Nenhum dado dessas trilhas é perdido. Os logs existentes são preservados mesmo quando as trilhas são removidas.
- O AWS Control Tower cria um caminho no mesmo bucket do Amazon S3 para as trilhas, a fim de diferenciar as trilhas no nível da conta das trilhas no nível da organização.
  - O caminho do log de trilhas da conta tem o seguinte formato: `/orgId/AWSLogs/...`
  - O caminho do log de trilhas da organização tem o seguinte formato: `/orgId/AWSLogs/orgId/...`
- CloudTrail Trilhas adicionais que você implantou, trilhas não implantadas pelo AWS Control Tower, não são tocadas.
- Todas as contas são incluídas na trilha no nível da organização, incluindo contas não inscritas no AWS Control Tower, caso as contas não inscritas façam parte de uma UO registrada.
- Os CloudWatch alarmes da Amazon em contas vinculadas não são acionados.
- Se você optar por cancelar uma trilha no nível da organização, o 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 no nível da organização

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

Considerar um ambiente de teste

Ao fazer upgrade da zona de pouso, o AWS Control Tower faz alterações somente nas contas compartilhadas e na UO fundamental. Ele não faz alterações em suas contas de carga de trabalho ou OUs. No entanto, como prática recomendada, ao operar o ambiente do AWS Control Tower, recomendamos configurar 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 serviços (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.

Lista de verificação para erros comuns ao atualizar

Aqui está uma pequena lista de tarefas que você pode realizar para evitar erros comuns ao atualizar sua zona de pouso do AWS Control Tower de versões 2.x para 3.x.

Lista de verificação básica de atualização

- Verifique sua landing zone:

  — Acesse o serviço AWS Control Tower, revise as páginas de unidades organizacionais e contas e confirme se o estado da sua conta está definido como Registrado e Registrado.

  — Se aplicável, verifique e confirme se a última execução do seu pipeline de personalizações foi bem-sucedida.

  — Verifique o bucket de registro centralizado do Amazon S3 na conta de auditoria, pois todas as alterações feitas anteriormente na política do bucket serão substituídas.
- Valide que qualquer SCPs pessoa que não seja de propriedade da AWS Control Tower não restringirá a `AWSControlTowerExecution` função de realizar ações nas contas dos membros ou ações na conta de gerenciamento da função administrativa que está executando a atualização.

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 políticas de SCP 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 políticas SCP de exclusão da IA podem ser aplicadas a toda a sua organização, a uma UO 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 equipe de administradores da nuvem central manter a zona de pouso atualizada. A atualização da zona de pouso garante que o AWS Control Tower seja corrigido e atualizado. Além disso, para proteger a zona de pouso de possíveis problemas de conformidade, os membros da equipe de administradores da nuvem central devem resolver problemas de desvios assim que eles forem detectados e relatados.

> **Note**
>
> O console do AWS Control Tower indica quando a zona de pouso precisa ser atualizada. Caso não haja uma opção para atualizar, é porque a zona de pouso 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.

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

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 atualiza a zona de pouso, você tem a oportunidade de modificar as configurações de zona inicial.

Benefícios da atualização

- É possível alterar suas regiões administradas
- É possível alterar sua política de retenção de logs
- É possível adicionar ou remover o controle de negação de região
- Você pode aplicar chaves de criptografia AWS KMS
- Você pode ativar ou desativar sua trilha no nível da organização CloudTrail .
- Você pode resolver o desvio da zona de pouso

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

Se uma atualização falhar, o AWS Control Tower não voltará para uma versão anterior da zona de pouso. Você pode encontrar a zona de pouso em um estado indeterminado. Em caso afirmativo, entre em contato com AWS o suporte. Consulte mais informações sobre como solucionar as falhas de atualização em Não é possível atualizar a zona de pouso.

Você tem a oportunidade de limpar mapeamentos não utilizados do AWS Identity Center (anteriormente chamado de AWS SSO) ao atualizar sua landing zone. Consulte mais informações em Field Notes: Clear Unused IAM Identity Center Mappings Automatically During AWS Control Tower Upgrades.

Pré-requisito para atualização e redefinição: desative o recurso pagamentos pelo solicitante

Antes de atualizar ou redefinir a zona de pouso, certifique-se de que o bucket de registro em log do Amazon S3 para a conta de arquivamento de logs não tenha o recurso Pagamentos pelo solicitante habilitado. Você deve desabilitar esse recurso antes de iniciar o processo de atualização ou redefinição. Quando o AWS Control Tower configura o bucket de registro em log, esse recurso não é habilitado. Portanto, somente os clientes que ativaram posteriormente o recurso pagamentos pelo solicitante 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 zona de pouso

São necessárias atualizações para corrigir o desvio de governança ou para mudar para uma nova versão do AWS Control Tower. Para executar uma atualização completa do AWS Control Tower, é necessário atualizar primeiro a zona de pouso e atualizar individualmente as contas inscritas. 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 Configurações de zona inicial. Talvez seja necessário executar uma atualização da zona de pouso para resolver determinados tipos de desvio, e é possível 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, acesse 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 UO ou com uma abordagem de script automatizada, descrita em uma seção posterior desta página.
- Uma atualização completa: uma atualização completa inclui uma atualização de sua landing zone, seguida por uma atualização de todas as contas inscritas em seu cadastro OUs. Atualizações completas são necessárias com uma nova versão do AWS Control Tower, como 3.0, 3.2 e assim por diante. Para facilitar o processo completo de atualização, pois OUs com 1.000 contas ou

menos, você pode escolher Registrar UO Novamente para atualizar todas as contas dentro dessa UO e repetir o comando Registrar UO Novamente para cada UO.

Para obter mais informações sobre atualizações da zona de pouso, consulte Melhores práticas para atualizações da zona de pouso.

> **Note**
>
> Depois de concluir uma atualização da zona de pouso, você não pode desfazer a atualização ou fazer downgrade para uma versão anterior.

Atualizar a zona de pouso

A maneira mais fácil de atualizar a zona de pouso do AWS Control Tower é por meio da página Configurações de zona inicial, que você pode acessar escolhendo Configurações de zona inicial no painel de navegação à esquerda do painel do AWS Control Tower.

A página Configurações de zona inicial mostra a versão atual da zona de pouso e lista as versões atualizadas que podem 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 orienta você pelas etapas de uma atualização completa para o AWS Control Tower pelo console. Para atualizar uma conta individual, consulte Atualizar a conta no console.

Para atualizar a zona de pouso, com qualquer número de contas por UO

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 backend da zona de pouso, bem como as contas compartilhadas. Esse processo pode demorar pouco mais de meia hora.
3. Atualize suas contas-membros (esse procedimento deve ser seguido para uma UO que contenha mais de mil contas).
4. No painel de navegação à esquerda, escolha Organização.
5. Para atualizar cada conta, siga as etapas fornecidas em Atualizar a conta no console.

> **Opcionalmente, registre novamente a UO para atualizar as contas**
>
> Para o AWS Control Tower registrado OUs com menos de 1.000 contas, você pode acessar a página da OU no painel e selecionar Registrar novamente a OU para atualizar as contas nessa OU.

Selecionar uma versão da zona de pouso

Se estiver executando a versão 3.1 ou posterior da zona de pouso do AWS Control Tower, você poderá optar por permanecer na versão atual ou fazer upgrade para uma versão mais recente ao realizar uma operação de Atualização ou Redefinição nas configurações da zona de pouso. A operação de Redefinição é a melhor maneira de reparar desvios, na maioria das situações.

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

> **Note**
>
> Se você optar por implantar uma versão da zona de pouso que pule uma versão intermediária, por exemplo, se você mudar de 3.1 para 3.3, o AWS Control Tower implantará automaticamente a versão intermediária como parte da operação de atualização.
> Em uma conversa, o ato de mudar para uma versão mais recente costuma ser chamado de upgrade, não apenas de atualização. Esses dois conceitos são distintos, pois você

pode atualizar as configurações de zona inicial sem precisar fazer upgrade para uma nova versão, por exemplo, alterando as regiões que você administra. No console, o botão Atualizar executa uma atualização no local ou uma operação de upgrade, com base na versão atual da zona de pouso e na que você escolheu para implantar.

Selecionar a versão da zona de pouso: procedimento do console

1. No console do AWS Control Tower, acesse a página de Configurações de zona inicial. 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 na tabela, é possível ver as ações disponíveis. A Atualização estará disponível se a versão atual for anterior à versão selecionada. A Redefinição estará disponível se a versão atual for a 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. Será exibida uma tela de confirmação mostrando a versão da zona de pouso que você selecionou para implantação. Para continuar, escolha Avançar no canto inferior direito. A operação de atualização pode levar alguns minutos ou mais.
5. Depois que a zona de pouso for atualizada, talvez seja necessário atualizar as 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 cadastrados OUs.

Atualizações da conta, versões da zona de pouso e linhas de base

As zonas de pouso do AWS 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. É possível visualizar uma tabela que mostra Compatibilidade das linhas de base da UO e das versões da zona de pouso.

Ao pular uma versão da linha de base, é necessário atualizar as contas após a atualização da zona de pouso. Por exemplo, ao atualizar de 3.1 para 3.2, não seria necessário atualizar as contas, porque essas versões da zona de pouso compartilham a mesma linha de base.

Por outro lado, ao atualizar de 3.1 para 3.3, seria necessário atualizar as contas, porque a versão da linha de base é 4.0, que abrange de 3.2 a 3.3.

Consulte mais informações sobre a relação entre as versões da zona de pouso e as linhas de base em Compatibilidade das linhas de base da UO e das versões da zona de pouso.

Mantenha as AWS CloudTrail trilhas durante a atualização da landing zone

Você pode optar por manter suas AWS CloudTrail trilhas no nível da conta ao atualizar sua versão da zona de pouso do AWS Control Tower.

Pré-requisitos

- Sua versão do landing zone é inferior a 3.0.
- Sua operação de criação ou atualização mais recente foi bem-sucedida.

Para manter a trilha em nível de conta e optar por trilhas em nível de organização CloudTrail

1. Entre em contato com o AWS Support solicitando que sua conta seja permitida na lista de permissões.
2. A equipe de suporte confirma quando a conta de destino está na lista de permissões.
3. Após a confirmação, atualize seu landing zone para a versão 3.1 ou superior e escolha AWS CloudTrail configuração - Ativado.

Para manter a trilha no nível da conta e optar por não participar das CloudTrail trilhas gerenciadas pelo AWS Control Tower

1. Entre em contato com o AWS Support solicitando que sua conta seja permitida na lista de permissões.
2. A equipe de suporte confirma quando a conta de destino está na lista de permissões.
3. Após a confirmação, atualize seu landing zone para a versão 3.1 ou superior e escolha AWS CloudTrail configuração - Não habilitado.

> **Important**
>
> Depois que as CloudTrail trilhas em nível de conta forem mantidas, não poderemos remover trilhas nem remover suas contas da lista de permissões.

Como fazer uma solicitação de suporte para manter suas trilhas no nível da conta

Se você precisar manter trilhas no nível da conta durante uma atualização da Landing Zone, entre em contato com o AWS Support para adicionar sua conta à lista de permissões do AWS Control Tower. Siga estas etapas para enviar um ticket de suporte:

1. Faça login no AWS Management Console.
2. Navegue até o AWS Support Center.
3. Escolha Criar caso.
4. Em Tipo de caso, selecione Suporte técnico.
5. Para Serviço, escolha AWS Control Tower.
6. Em Categoria, selecione Orientação geral.
7. Na linha de assunto, inclua a seguinte frase:

   ```
   Allow retention of account-level trails during Landing Zone update
   ```
8. No campo Descrição, forneça os seguintes detalhes:
   - O número AWS da sua conta de gerenciamento
   - A região de origem selecionada para seu ambiente do AWS Control Tower
9. Preencha todos os outros campos obrigatórios no formulário do caso de suporte.
10. Escolha Enviar para criar o caso de suporte.

Depois de enviar o ticket, o AWS Support analisa sua solicitação e adiciona sua conta à lista de permissões, se apropriado. Você receberá mais instruções e confirmações por meio do canal de comunicação do caso de suporte.

> **Note**
>
> Para excluir a trilha no nível da conta depois que ela estiver na lista de permissões, use a conta de gerenciamento para excluir o conjunto de pilhas ou a AWS CloudFormation instância específica da pilha. Todos os recursos na pilha são excluídos.

Resolver o desvio com a redefinição e o novo registro

O desvio geralmente ocorre quando você e os membros da sua organização usam a zona de pouso.

A detecção de desvios é automática no 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 vários tipos de deriva, escolha Redefinir na página de configurações da zona de pouso no console. Além disso, você pode resolver alguns tipos de desvio escolhendo registrar novamente uma OU no console. Para controles, você pode resolver o desvio programaticamente chamando a API. ResetEnabledControl Consulte mais informações sobre os tipos de desvio e como resolvê-los em Tipos de deriva de governança e Detectar e resolver desvios no AWS Control Tower.

Um caso especial de resolução de desvio ocorre para o desvio de perfil. Se um perfil necessário não estiver disponível, o console mostrará uma página de aviso e algumas instruções sobre como restaurar o perfil. A zona de pouso não estará disponível até que a mudança de perfil seja resolvida. Essa redefinição do desvio não é a mesma que uma redefinição completa da zona de pouso. Consulte mais informações em Não exclua os perfis necessários na seção chamada Tipos de desvio a serem resolvidos imediatamente.

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

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

Provisionar e atualizar contas usando automação

É possível provisionar ou atualizar contas individuais no AWS Control Tower por vários métodos:

- É possível provisionar e personalizar contas com o Account Factory for Terraform (AFT) do AWS Control Tower. Para obter mais informações, consulte Visão geral do Account Factory for Terraform (AFT) do AWS Control Tower.

- É possível atualizar contas com o Customizations for AWS Control Tower (CfCT). Para obter mais informações, consulte Visão geral do Customizations for AWS Control Tower (CfCT) .
- Automação de scripts: se preferir usar uma abordagem de API, você poderá atualizar as contas usando o framework de API do Service Catalog e a AWS CLI para atualizar as contas em um processo em lote. Você chamaria a API `UpdateProvisionedProduct` do Service Catalog para cada conta. Você pode escrever um script para atualizar as contas, uma por uma, com esta API. 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 aguardar o êxito de pelo menos uma atualização antes de iniciar a próxima atualização de 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 by Service Catalog APIs.

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

Uma etapa adicional da automação por script é verificar o status de Sucesso do evento de ciclo de vida `UpdateLandingZone` do 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 uma atualização da zona de pouso está 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.
- Automatizar tarefas no AWS Control Tower .

Automatizar tarefas no AWS Control Tower

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

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

A página Mais informações e links contém links para muitas publicações de blog técnicas excelentes que podem ajudar 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 ajudar a automatizar tarefas.

Automatizar tarefas de controle

É possível automatizar tarefas relacionadas à aplicação e remoção de controles (também conhecidos como barreiras de proteção) por meio da API do AWS Control Tower. Consulte detalhes na Referência de API do AWS Control Tower.

Para obter mais informações sobre como realizar operações de controle com a AWS Control Tower APIs, consulte a postagem no blog AWS Control Tower lança a API, controles predefinidos para suas unidades organizacionais.

Automatizar as tarefas da zona de pouso

A zona de pouso do AWS Control Tower APIs ajuda você a automatizar determinadas tarefas relacionadas à sua zona de pouso. Consulte detalhes na Referência de API do AWS Control Tower.

Automatizar o registro de UO

A linha de base do AWS Control Tower APIs ajuda você a automatizar determinadas tarefas, como registrar uma OU. Consulte detalhes na Referência de 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 obter mais informações, consulte Encerrar uma conta-membro do AWS Control Tower por meio do 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 é possível criar contas e atualizá-las repetidamente, depois de configurar um único esquema, 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 obter mais informações, consulte Provisionar contas com o Account Factory for Terraform (AFT) do AWS Control Tower .

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, políticas de controle de serviços (SCPs) e políticas de controle de recursos (RCPs). Para obter mais informações, consulte Visão geral do Customizations for AWS Control Tower (CfCT) .

Consulte mais informações e um vídeo sobre o provisionamento automatizado de contas em Walkthrough: Automated account provisioning in AWS Control Tower e Automated provisioning with IAM roles.

Consulte também Update accounts by script.

Auditoria programática de contas

Consulte mais informações sobre a auditoria programática de contas em Programmatic roles and trust relationships for the AWS Control Tower audit account.

Automatizar outras tarefas

Consulte informações sobre como aumentar determinadas cotas de serviços do AWS Control Tower com um método de solicitação automatizado neste vídeo: Automate Service Limit Increases.

Para blogs técnicos que abordam casos de uso de automação e integração, consulte Automation and integration.

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. Ela também ilustra como excluir a VPC padrão em cada região.

A arquitetura de referência de segurança da AWS 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 da APIs 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 na AWS CLI — é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do. AWS Management Console Não há necessidade de baixar nem instalar ferramentas da 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 permissões do IAM para AWS CloudShell

AWS Identity and Access Management fornece recursos de gerenciamento de acesso que permitem que os administradores concedam permissões aos usuários do IAM e 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 identidades do IAM:

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

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

> **Note**
>
> Sua identidade do IAM também exige uma política que conceda permissão para fazer chamadas ao 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 fez a autenticação no shell, então não precisará 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 destino e estar conectado como um usuário do IAM Identity Center ou do IAM com permissões administrativas para a conta de gerenciamento que contém sua zona de destino.

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

   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)
- Managing the Delivery Channel

3. Este exemplo mostra os comandos da AWS CLI que você inseriria AWS CloudShell para habilitar ou desabilitar 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 serviço confiável

   - `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 método PutObject.

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

Se o upload do objeto é feito com sucesso no bucket do Amazon S3, a linha de comando exibe uma resposta do serviço semelhante à seguinte saída:

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

O `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 ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation 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 Consulte mais informações, como exemplos de modelos JSON e YAML para esses tipos de recursos em AWS Control Tower no Guia do usuário do AWS CloudFormation .

> **Note**
>
> O limite `EnableControl` e as `DisableControl` atualizações AWS Control Tower são de 100 operações simultâneas.

Para ver alguns AWS Control Tower exemplos da 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
- Referência de API do AWS CloudFormation
- AWS CloudFormation Guia do usuário da interface de linha de comando

Personalizar a zona de pouso do AWS Control Tower

Certos aspectos da 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.

Personalizar pelo console do AWS Control Tower

Para fazer essas personalizações na zona de pouso, siga as etapas fornecidas pelo console do AWS Control Tower.

Selecionar nomes personalizados durante a configuração

- Você pode selecionar seus nomes de UO de nível superior durante a configuração. Você pode renomear seu OUs a qualquer momento usando o AWS Organizations console, mas fazer alterações OUs em seu IN AWS Organizations pode causar desvios reparáveis.
- Você pode selecionar os nomes das suas contas compartilhadas de Auditoria e Arquivamento de logs, 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 UO por meio do AWS Control Tower, incluindo criar, excluir ou registrar novamente uma UO.

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.

Personalizar adicionando controles opcionais

- Os controles altamente recomendáveis e eletivos são opcionais, o que significa que é possível personalizar o nível de imposição para a zona de pouso escolhendo quais habilitar. Os controles opcionais não são habilitados por padrão.
- Os controles de residência de dados opcionais permitem que você personalize as regiões nas quais você armazena e permite o acesso aos seus dados.
- Os controles opcionais que fazem parte do padrão integrado do Security Hub permitem verificar seu ambiente do AWS Control Tower em busca de 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 a zona de pouso. O AWS Control Tower cria uma trilha no nível da organização 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.

Criar contas-membros personalizadas no console

- Você pode criar contas-membros do AWS Control Tower que são personalizadas e pode atualizar contas-membros existentes para adicionar personalizações, pelo AWS Control Tower. Para obter mais informações, consulte Personalizar contas com Account Factory Customization (AFC).

Automatizar 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 do Terraform, disponível no repositório do 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.

- Você pode personalizar a zona de pouso do AWS Control Tower com o Landing Zone Accelerator (LZA) na AWS. A solução LZA foi projetada para se alinhar às AWS melhores práticas e estar em conformidade com várias estruturas globais de conformidade. Recomendamos que você implante o AWS Control Tower como a zona de pouso fundamental e, depois, aprimore os recursos da zona de pouso com o LZA, conforme necessário. Consulte mais informações em AWS Control Tower and Landing zone accelerator.

AWS Control Tower e acelerador da zona de pouso

Esta seção descreve os benefícios de trabalhar em conjunto com o AWS Control Tower e a solução Landing Zone Accelerator (LZA).

Você pode personalizar a zona de pouso do AWS Control Tower com o Landing Zone Accelerator (LZA) na AWS .

O LZA é uma solução que implanta um conjunto básico de recursos projetados para se alinhar às AWS melhores práticas e a várias estruturas globais de conformidade, para ajudar você a gerenciar e governar um ambiente com várias contas. O LZA é criado usando o AWS Cloud Development Kit (CDK).

O LZA configura automaticamente um ambiente de nuvem adequado para hospedar workloads seguras. Essa solução pode ser implantada em todos Regiões da AWS, para ajudá-lo a manter a consistência das operações e da governança. A solução LZA foi projetada para se alinhar às AWS melhores práticas e estar em conformidade com várias estruturas globais de conformidade.

Recomendamos que você implante o AWS Control Tower como sua zona de pouso fundamental e, depois, aprimore seus recursos de zona de pouso com o LZA, conforme necessário. A combinação do LZA e do AWS Control Tower fornece uma solução abrangente e sem código que ajuda você a gerenciar e governar um ambiente de várias contas. Ela foi criada para comportar workloads altamente regulamentadas e requisitos complexos de conformidade. Juntos, o AWS Control Tower e o Landing Zone Accelerator ajudam você a estabelecer a prontidão da plataforma, incluindo recursos operacionais, de segurança e conformidade.

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

Consulte mais informações sobre como combinar o LZA e o AWS Control Tower no guia de implementação do LZA.

Benefícios do Customizations for AWS Control Tower (CfCT)

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

Esse processo de infrastructure-as-codepersonalização integra AWS CloudFormation modelos com políticas de controle de AWS serviço (SCPs) e eventos de ciclo de vida do AWS Control Tower, para que suas implantações de recursos permaneçam sincronizadas com sua landing zone. Por exemplo, ao criar uma conta com o Account Factory, os recursos anexados à conta e à UO 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 a sua landing zone, implantando os 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 implantar 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 nas contas e OUs, automaticamente.
- Estenda a arquitetura de rede: você pode implantar arquiteturas de rede personalizadas que melhoram e protegem sua conectividade, como um gateway de trânsito.

Exemplos adicionais do 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 segurança da AWS , no repositório `aws-samples`. Muitos desses exemplos contêm arquivos `manifest.yaml` 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 do Customizations for 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 do CfCT é integrado aos eventos do ciclo de vida do AWS Control Tower, para que suas implantações de recursos permaneçam sincronizadas com a zona de pouso. Por exemplo, quando uma conta é criada com o Account Factory, todos os recursos anexados 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 práticas recomendadas para implantar um pipeline escalável do CfCT e personalizações comuns de CfCT.

A seção a seguir fornece considerações arquitetônicas e etapas de configuração para a implantação do Customizations for AWS Control Tower (CfCT). 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 de infraestrutura de TI e desenvolvedores com experiência prática em arquitetura na Nuvem AWS .

Para obter informações sobre as últimas atualizações e alterações nas personalizações do AWS Control Tower (cFCT), consulte o arquivo CHANGELOG.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.

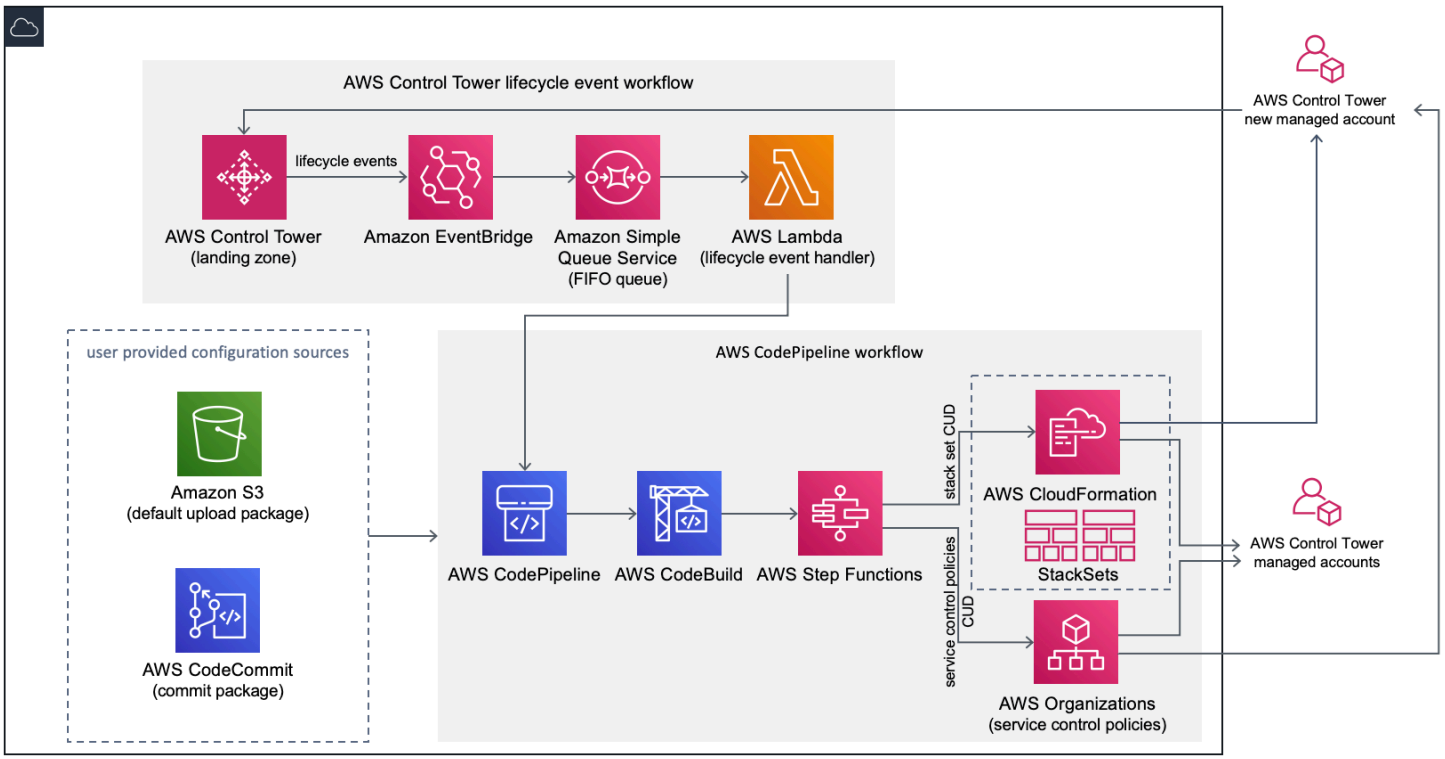

Figura 1: Personalizações para a arquitetura do AWS Control Tower

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

> **Observação**
>
> O CfCT deve ser implantado na região de origem do AWS Control Tower e na conta de gerenciamento do AWS Control Tower, porque é aí que a zona de pouso do AWS Control Tower é implantada. Consulte informações sobre como configurar uma zona de pouso do AWS Control Tower em Conceitos 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. Consulte mais informações em Configurar o Amazon S3 como fonte de configuração.

O CfCT implanta dois fluxos de trabalho:

- um fluxo de trabalho do AWS CodePipeline
- e um fluxo de trabalho de eventos do ciclo de vida do AWS 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.

Ao fazer upload do pacote de configuração, o CfCT invoca o pipeline de código para executar três estágios.

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

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

> **Observação**
>
> Consulte informações detalhadas sobre a personalização do pacote de configuração em Guia de personalização do CfCT.

O fluxo de trabalho de eventos do ciclo de vida do AWS 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 (FIFO) do Amazon Simple Queue Service (Amazon SQS) e uma função. AWS Lambda

Quando a regra de eventos da Amazon detecta um EventBridge evento de ciclo de vida correspondente, ela passa o evento para a fila FIFO do Amazon SQS, 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 será de USD 3 por mês. Consulte detalhes completos na página de preços de cada serviço da AWS 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, a cobrança será feita 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 detalhes sobre preços do Amazon S3 e do AWS CodeCommit.

Serviços de componentes

Os AWS serviços a seguir são componentes das personalizações do 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 Consulte informações sobre compatibilidade de versões em Setting up for 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 Consulte mais informações sobre o controle da fonte de configuração em Usar 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 Consulte mais informações sobre os estágios do pipeline em Guia de personalização do CfCT.

AWS Key Management Service

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

AWS Lambda

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

Amazon Simple Notification Service

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

Amazon Simple Storage Service

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

Exemplo: o nome do bucket do Amazon S3

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

O bucket contém um arquivo de amostra 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.

Consulte informações sobre a personalização do arquivo de configuração em Guia de personalização do CfCT.

Amazon Simple Queue Service

O cFct usa uma fila FIFO do Amazon Simple Queue Service (Amazon SQS) para capturar 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 sobre SCPs, consulte AWS Organizations.

AWS Step Functions

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

AWS Armazenamento de parâmetros do Systems Manager

O AWS 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

Inicie o Customizations for AWS Control Tower (CfCT) na mesma conta e região em que sua zona de pouso do AWS Control Tower está implantada; ou seja, você deve implantá-lo na conta de gerenciamento do AWS Control Tower na sua região de origem do AWS Control Tower. Por padrão, o CfCT cria e executa o pacote de configuração da zona de pouso 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. É possível escolher a fonte de configuração e permitir a aprovação manual das implantações do pipeline. As duas seções a seguir apresentam mais detalhes sobre essas opções.

Escolher 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 na forma de um arquivo `.zip` 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. Consulte informações sobre a atualização do pacote de configuração em Usar 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. Ao terminar de personalizar o pacote de configuração, faça upload de `custom-control-tower-configuration.zip` sem o sublinhado (_) para iniciar a implantação no 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.

> **Compactar ou não compactar?**
>
> Ao usar o bucket padrão do S3, o pacote de configuração deve estar disponível como um arquivo `.zip`. Se você estiver usando o repositório do AWS CodeCommit , coloque 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.

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

Escolher seus parâmetros de aprovação da configuração do pipeline

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

Quando a aprovação manual é habilitada, o pipeline de configuração valida as personalizações feitas no manifesto e nos modelos de arquivos do AWS Control Tower e, depois, 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).

É possível 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.

Como atualizar o Customizations for AWS Control Tower

Se você já implantou o cFCT, deve atualizar a AWS CloudFormation pilha para obter a versão mais recente da estrutura do cFCT. Consulte detalhes em 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 do AWS Control Tower.

Tempo para implantação: aproximadamente 15 minutos

Pré-requisitos

O CfCT deve ser implantado na sua conta de gerenciamento do AWS Control Tower e na sua região de origem do AWS Control Tower. Se você não tiver uma zona de pouso configurada, consulte Conceitos 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

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

Etapa 2. Criar um pacote personalizado

- Crie um pacote de configuração personalizada.

> **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

O AWS CloudFormation modelo nesta seção implanta personalizações para o AWS Control Tower (cFct) em sua conta.

> **Observação**
>
> Você é responsável pelo custo dos AWS serviços usados enquanto executa o cFct. Consulte mais detalhes em Custo.

1. Para iniciar personalizações para o AWS Control Tower, faça o download do 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 iniciado na mesma região e conta em que você implantou a zona de pouso do AWS Control Tower, que é sua região de origem.

3. Na página Criar pilha, verifique se o URL de modelo correto é exibido na caixa de texto URL e selecione Próximo.
4. Na página Especificar detalhes da pilha, atribua um nome para a pilha do CfCT.
5. Em Parâmetros, revise os parâmetros a seguir e modifique-os no modelo, se necessário.

Configuração do pipeline		
Parameter	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	<Entrada opcional>	O endereço de e-mail para notificações de aprovação

Configuração do pipeline		
Parameter	Padrão	Descrição
		. Para usar esse parâmetro , é necessário definir o parâmetro Estágio de aprovação do pipeline como `Yes`.
CodePipelineFonte da AWS	`Amazon S3`	A fonte da AWS CodePipel ine para ajudá-lo a seleciona r onde armazenar e configurar as personali zações do cFct.
CodeCommit Configuração da AWS		
Parameter	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 defina o parâmetro `Yes` e insira o nome exato desse repositório.

CodeCommit Configuração da AWS		
Parameter	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		
Parameter	Padrão	Descrição
Tipo de simultaneidade 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 de simultaneidade máxima	`100`	A porcentagem máxima de contas em que essa operação pode ser executada ao mesmo tempo. O valor máximo permitido é 100. Consulte mais informações em Operações do conjunto de pilhas.

AWS CloudFormation StackSets Configuração		
Parameter	Padrão	Descrição
Porcentagem de tolerância a falhas	`10`	A porcentagem de contas, por região, nas quais essa operação de pilha pode falhar antes que a AWS CloudFormation interrompa a operação nessa região. O valor mínimo permitido é 0 e o valor máximo permitido é 100. Consulte mais informações em Operações do conjunto de pilhas.

6. Escolha Próximo.
7. Na página Configurar opções de pilha, selecione Avançar.
8. Na página Revisar, verifique e confirme as configurações. Não se esqueça de marcar a caixa de seleção confirmando que o modelo criará recursos do 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 deverá ver um status de CREATE_COMPLETE em cerca de 15 minutos.

Etapa 2. Criar um pacote personalizado

Com a pilha lançada, você pode adicionar personalizações à sua zona de pouso e às políticas de controle de serviços (SCPs) do AWS Control Tower personalizando o pacote de configuração incluído. Consulte instruções detalhadas sobre como criar um pacote personalizado no Guia de personalização do CfCT.

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

Atualizar a pilha

Se você já implantou personalizações para o 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). Consulte instruções sobre como começar a usar o Amazon S3 em Conceitos básicos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

1. Faça login no console do AWS CloudFormation.
2. Selecione suas personalizações atuais para a CloudFormation pilha do AWS Control Tower (cFct) e, em seguida, selecione Atualizar.
3. Em Pré-requisito: preparar modelo, selecione Substituir o modelo atual.
4. Na página Especificar modelo, faça o seguinte:
   a. Em Fonte do modelo, selecione Substituir modelo atual.
   b. Para o URL do Amazon S3, insira o URL do modelo do qual você fez o upload anteriormente para o Amazon S3 e, em seguida, escolha Avançar. GitHub
   c. Verifique se o URL do modelo está correto. Depois, selecione Próximo e Próximo novamente.
5. Em Parâmetros, revise os parâmetros do modelo e modifique-os conforme necessário. Consulte detalhes sobre os parâmetros na Etapa 1. Inicie a pilha.
6. Escolha Próximo.
7. Na página Configurar opções de pilha, selecione Avançar.
8. Na página Revisar, verifique e confirme as configurações. Você deve selecionar a caixa de seleção confirmando que o modelo cria os recursos do 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 receber o status UPDATE_COMPLETE em cerca de 15 minutos.

Excluir um conjunto de pilhas

É possível excluir um conjunto de pilhas se tiver habilitado 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 realizada para excluir o conjunto de pilhas associado quando um recurso é removido do arquivo de manifesto do CfCT.

Se você alterar o valor de `enable_stack_set_deletion` para `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 compatível com a 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, TODOS os recursos que começam com o prefixo `CustomControlTower-`, que têm a tag de chave `Key:AWS_Solutions, Value: CustomControlTowerStackSet` associada e que não são declarados no arquivo de manifesto, são preparados para exclusão.

Veja a seguir um exemplo de como definir esse parâmetro em um arquivo `manifest.yaml`:

```
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
```

Definir o Amazon S3 como fonte de configuração

Ao configurar o Customizations for AWS Control Tower, ele armazena um arquivo de configuração inicial, chamado `_custom-control-tower-configuration.zip`, 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 `custom-control-tower-configuration.zip` e, depois, enviá-lo de volta ao 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, é necessário atualizar a política de chave do KMS para especificar os perfis que devem receber acesso. O perfil pode ser de administrador, usuário ou ambos. Siga este procedimento:

1. Navegue até o console do AWS Key Management Service.
2. Em Chaves gerenciadas pelo cliente, selecione CustomControlTowerKMSKey.
3. Selecione a guia Política de chave. Depois, selecione Editar.

4. Na página Editar política de chave, encontre a seção Permitir o uso da chave no código e adicione uma destas permissões:
   - Como adicionar um perfil administrativo:

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

     `arn:aws:iam::<account-ID>:user/<username>`
5. Escolha Salvar alterações.
6. Acesse o console do Amazon S3, encontre o bucket do S3 que contém o arquivo zip de configuração e selecione “download”.
7. Faça as alterações de configuração necessárias no arquivo de manifesto e nos arquivos de modelo. Consulte informações sobre como personalizar os arquivos de manifesto e de modelo em the section called “Guia de personalização do CfCT”.
8. Faça upload das 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`

Configurar GitHub como fonte de configuração

Esta seção explica como implantar personalizações para o AWS Control Tower (cFCT) GitHub como fonte. O processo tem três etapas principais:

- Prepare um GitHub repositório
- Crie a conexão GitHub de código
- Implante a AWS CloudFormation pilha

Prepare um GitHub repositório

Crie um repositório em sua GitHub conta, o nome padrão usado no modelo é`custom-control-tower-configuration`. Considere tornar o repositório de destino privado. Você definirá suas personalizações em um `yaml` arquivo chamado `manifest.yaml` na pasta de implantação do repositório cFct.

O guia de personalização do cFct fornece orientações detalhadas sobre como criar um `manifest.yaml` para configurar suas personalizações.

Crie a GitHub conexão

Na sua instância Developer Tools --Connections para Github, execute as seguintes etapas:

1. Selecione Criar conexão e escolha GitHub como provedor
2. Escolha Criar uma conexão de GitHub aplicativo e, no campo Nome da conexão, insira GitHub cFct ou qualquer nome que você escolher
3. Selecione Conectar a GitHub e escolha Instalar um novo aplicativo
4. Selecione o GitHub usuário ou a organização do seu repositório
5. Em Acesso ao repositório, escolha Somente selecionar repositórios, selecione o repositório que você criou anteriormente e Salve seu trabalho.
6. Observe o ARN das conexões de código - você precisará dele ao implantar a pilha. AWS CloudFormation

Implante a AWS CloudFormation pilha

- Baixe o `custom-control-tower-initiation.template` arquivo do repositório.
- Crie uma nova AWS CloudFormation pilha usando o `custom-control-tower-initiation.template` arquivo.
- Em AWS CodePipeline Fonte, escolha GitHub (via Conexão de Código).
- Em GitHub Configuração, especifique estes campos:
  - Para o ARN da Conexão de Código, forneça o ARN da Conexão de Código
  - para GitHub Usuário ou Organização, forneça o nome do GitHub usuário ou organização sob a qual você criou o repositório
  - Em Nome GitHub do repositório, insira o nome do repositório (o padrão é) `custom-control-tower-configuration`
  - Em Nome GitHub da filial, insira o nome da filial (o padrão é) `main`

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/hora: carimbo de data/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 Política de Privacidade da AWS.

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`** do 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 da AWS Control Tower para suas empresas e clientes. Ele fornece informações sobre a personalização e a extensão do ambiente do AWS Control Tower com o pacote de personalização do 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 procedimento 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 complementar
- Outros arquivos JSON para descrever e implementar suas personalizações de ambiente do AWS Control Tower

Por padrão, o pacote de configuração `_custom-control-tower-configuration.zip` 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 complementar e outros arquivos JSON
- realiza validações de manifesto e modelo
- invoca seções no arquivo de manifesto cFct 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 inicia o AWS CodePipeline automaticamente.

Lembre-se do sublinhado

O nome do arquivo do pacote de configuração de amostra começa com um sublinhado (_) para que o AWS CodePipeline não seja acionado automaticamente. Ao concluir a personalização do pacote de configuração, faça upload do arquivo `custom-control-tower-configuration.zip` sem o sublinhado (_) para acionar a implantação no AWS CodePipeline.

AWS CodePipeline estágios

O pipeline do cFct requer vários AWS CodePipeline estágios para implementar e atualizar seu ambiente do 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 compilação

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 manifesto e os modelos do AWS CloudFormation passarem nos testes, o pipeline continuará para o próximo estágio. 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)

   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 Estágio de aprovação do pipeline como Sim ao iniciar a pilha.

4. Estágio político

   O estágio da política invoca a máquina de estado da política de controle de serviço (SCP) ou da política de controle de recursos (RCP) para chamar AWS Organizations APIs essa criação ou. SCPs RCPs

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 do AWS Control Tower com o arquivo de manifesto cFct, o conjunto de modelos que o acompanha e outros arquivos JSON. Você empacotará esses arquivos em uma estrutura de pastas e os colocará no bucket do Amazon S3 como um arquivo `.zip`, 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 arquivo `custom-control-tower-configuration.zip` e faça upload somente do arquivo `.zip` 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 cFct

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

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

resources:
  #set of CloudFormation resources, SCP policies, or RCP 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. Veja a seguir as definições dessas palavras-chave.

região: uma string de texto para a região padrão do 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 de origem do AWS Control Tower é o padrão quando você cria recursos personalizados do 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 compatível mais recente é 2021-03-15.

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

> **Note**
>
> É altamente recomendável usar a versão mais recente. Para atualizar as propriedades do manifesto na versão mais recente, consulte Atualizações de versão para o manifesto cFct.

A próxima palavra-chave mostrada no exemplo anterior é recursos. 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 cFct

Este tópico descreve a seção de recursos do arquivo de manifesto cFct, na qual você definirá os recursos necessários para suas personalizações. Essa seção do arquivo de manifesto cFct começa nos recursos da palavra-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 e RCPs, qual cFct implanta automaticamente por meio do pipeline de código. Você pode listar OUs, contas e regiões para implantar instâncias de pilha.

As instâncias Stack são implantadas no nível da conta em vez do nível da OU. SCPs e RCPs são implantados no nível da OU. Consulte mais informações em Build your own customizations.

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 | rcp
    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.

- Tipo: 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.

- Tipo: string
- Obrigatório: não

resource_file — Esse arquivo pode ser especificado como a localização relativa do arquivo manifesto, um URI ou URL do Amazon S3 que aponta para um AWS CloudFormation modelo ou política de controle de AWS Organizations serviço em JSON para criar recursos, ou. AWS CloudFormation SCPs RCPs

- Tipo: 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 URI do Amazon S3.

```
resources:
  - name: SecurityRoles
    resource_file: s3://amzn-s3-demo-bucket/[key-name]
```

3. O exemplo a seguir mostra o arquivo de recurso fornecido como um URL HTTPS do Amazon S3.

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Se você fornecer um URL do Amazon S3, verifique se a política do bucket permite acesso de leitura para a conta de gerenciamento do AWS Control Tower pela qual você está implantando o CfCT. Se você fornecer um URL HTTPS do Amazon S3, verifique se o caminho usa notação de pontos. Por exemplo, `.S3.us-west-1` O CfCT não é compatível com 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 em que os recursos estão 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 a *AccountId* variável mostrada no exemplo pelo ID da AWS conta de gerenciamento que está implantando o cFct. Consulte mais exemplos em Exemplos de políticas de bucket do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

parâmetros: especifica o nome e o valor dos parâmetros do AWS CloudFormation .

- Type MapList:
- Obrigatório: não

A seção de parâmetros contém pares de parâmetros de chave/valor. O pseudomodelo a seguir descreve a seção de parâmetros.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key: a chave associada ao parâmetro.
  - Tipo: 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.
  - Tipo: string
  - Obrigatório: sim (na propriedade de parâmetros)

deploy_method: o método de implantação para implantar recursos na conta. Atualmente, deploy_method suporta a implantação de recursos usando a `stack_set` opção de implantação de recursos por meio de AWS CloudFormation StackSets, a `scp` opção se você estiver implantando SCPs ou a `rcp` opção se estiver implantando. RCPs

- Tipo: string
- Valores válidos: `stack_set` | `scp` | `rcp`

- 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 um SCP ou RCP, o destino deve ser uma OU, não uma conta.

- Tipo: lista de strings `account name` ou `account number` para indicar que esse recurso será implantado em determinada lista de contas ou `OU names` para indicar que esse recurso será implantado em determinada lista de UOs.
- Obrigatório: pelo menos uma de accounts or organizational_units.
  - accounts:

    Tipo: lista de strings `account name` ou `account number` para indicar que esse recurso será implantado na lista de contas especificada.
  - organizational_units:

    Tipo: lista de strings `OU names` para indicar que esse recurso será implantado em uma lista de UOs especificada. Se você fornecer uma UO que não contenha contas e a propriedade de accounts 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, por padrão. Se você tiver um caso de uso especial, consulte Root OU.

export_outputs: lista de pares de nome/valor que denotam chaves de parâmetros do SSM. Essas chaves de parâmetros do SSM permitem que você armazene as saídas do modelo no armazenamento de parâmetros do SSM. 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: uma lista de pares de nome e valor. O nome contém a string `name` de uma chave de armazenamento de parâmetros do SSM e o valor contém string `value` do parâmetro.
- Valores válidos: qualquer string ou `$[output_`*`CfnOutput-Logical-ID`*`]` variável que *`CfnOutput-Logical-ID`* corresponda 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 da saída `VPCID` do modelo na chave de parâmetro do SSM chamada `/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 poderá 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 permite Raiz como um valor para uma unidade organizacional (UO) em `organizational_units` na versão V2 do manifesto (2021-03-15).

- Se você escolher o método de implantação de `scp` ou`rcp`, ao adicionar Root under`organizational_units`, o AWS Control Tower aplicará as políticas a todos os itens OUs sob o Root. Se você escolher o método de implantação de `stack_set`, ao adicionar Raiz em`organizational_units`, o CfCT implantará os conjuntos de pilhas em todas as contas na Raiz que estão inscritas no AWS Control Tower, exceto na conta de gerenciamento.
- De acordo com as práticas recomendadas do AWS Control Tower, a conta de gerenciamento se destina apenas a gerenciar contas-membros e para fins de cobrança. Não execute workloads de produção na conta de gerenciamento do AWS Control Tower.

  De acordo com a orientação de práticas recomendadas, 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 práticas recomendadas 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 accounts como destino de implantação e especifique a conta de gerenciamento. Caso contrário, não inclua accounts como destino da implantação. Você deve criar os recursos que faltam, incluindo os perfis do IAM necessários, 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 accounts como destino da implantação.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> O recurso UO raiz é compatível somente com a versão V2 do arquivo de manifesto (2021-03-15). Se você adicionar Root como UO em`organizational_units`, não adicione nenhuma outra OUs.

UO 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` ou`rcp`, o AWS Control Tower implanta o SCPs or RCPs na última OU no caminho aninhado da OU. Para o método de implantação `stack_set`, o AWS Control Tower implanta os conjuntos de pilhas em todas as contas na última UO no caminho aninhado da UO.

Por exemplo, considere o caminho `OUName1:OUName2:OUName3`. A última UO no caminho é `OUName3`. O cFct implanta os conjuntos RCPs de SCPs ou para `OUName3` e empilha 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 UO aninhada é compatível somente com a 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 cFct adicionando ou atualizando políticas de controle de serviço (SCPs), políticas de controle de recursos (RCPs) e recursos. AWS CloudFormation 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 arquivo `manifest.yaml`.

Esta seção explica as duas partes principais da como criar suas próprias personalizações:

- como configurar o 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 SCPs ou RCPs

Esta seção explica como criar um pacote de configuração para políticas de controle de serviços (SCPs) ou políticas de controle de recursos (RCPs). As duas partes principais desse processo são (1) preparar o arquivo de manifesto cFct e (2) preparar sua estrutura de pastas.

Etapa 1: edite o arquivo manifest.yaml

Use o arquivo `manifest.yaml` de amostra como ponto de partida. Insira todas as configurações necessárias. Adicione detalhes de `resource_file` e `deployment_targets`.

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 a mesma que a região do AWS Control Tower.

Para adicionar um SCP ou RCP personalizado na `example-configuration` pasta do pacote zip armazenado no bucket do Amazon S3, abra o arquivo e comece `example-manifest.yaml` 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 | rcp
    #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 | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

Etapa 2: crie uma estrutura de pastas

Você pode pular essa etapa se estiver usando um URL do Amazon S3 para o arquivo de recursos e se estiver usando parâmetros com pares de chave/valor.

Você deve incluir uma política SCP ou uma política RCP no formato JSON para oferecer suporte ao manifesto, pois o arquivo do manifesto faz referência ao arquivo JSON. Os caminhos do arquivo devem corresponder às informações de caminho fornecidas no arquivo de manifesto.

- Um arquivo JSON de política contém o SCPs ou RCPs para 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 política `block-s3-public.json`.

```
{
   "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: edite 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 para SCPs ou. RCPs 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 | rcp
    #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 detalhes de `resources`. A ordem de `resources` determina a ordem de execução para criar dependências de `resources`. Você pode editar o seguinte exemplo de arquivo de manifesto de acordo com suas necessidades empresariais.

```
---
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 | rcp
    #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: atualize a estrutura de pastas

Ao atualizar a estrutura de pastas, você pode incluir todos os arquivos de AWS CloudFormation modelo de suporte e arquivos de política SCP ou RCP 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 SSM Parameter Store definida no modelo. AWS CloudFormation Usando o auxiliar alfred, você pode usar valores armazenados no SSM Parameter Store sem atualizar o modelo. AWS CloudFormation Para obter mais informações, consulte O que é um AWS CloudFormation modelo? no Guia do AWS CloudFormation usuário.

> **Important**
>
> O auxiliar alfred tem duas limitações. Os parâmetros estão disponíveis somente na região de origem da conta de gerenciamento do AWS Control Tower. Como prática recomendada, considere trabalhar com valores que não mudam de uma instância de pilha para outra. 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 o `subnet ID` devem ser passados ao conjunto de pilhas 2 como valores de parâmetros. Antes que o `VPC ID` e o `subnet ID` possam ser passados ao conjunto de pilhas 2, o `VPC ID` e o `subnet ID` devem ser armazenados no conjunto de pilhas 1 usando `AWS::SSM::Parameter`. Consulte mais informações em `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 Consulte mais informações em `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]"
```

Esquema JSON para o pacote de personalização

O esquema JSON para o 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 arquivo cFct`manifest.yaml`.

Atualizações de versão para o manifesto cFct

Para obter informações sobre a versão mais recente de Customizations for AWS Control Tower (cFct), consulte o `CHANGELOG.md`arquivo no repositório. GitHub

> **Warning**
>
> A versão 2.2.0 de Customizations for AWS Control Tower (cFct) introduziu um esquema de manifesto cFct (versão 2021-03-15) para se alinhar ao serviço relacionado. AWS APIs O esquema do manifesto permite que um único arquivo manifest.yaml gerencie recursos compatíveis (AWS CloudFormation modelos e RCPs) por meio de fluxos de trabalho SCPs desacoplados. DevOps
> É altamente recomendável que você atualize o esquema do manifesto cFct da versão 2020-01-01 para a versão 2021-03-15 ou posterior.
> O CfCT mantém a compatibilidade com as 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 no Fim do suporte. Não fornecemos mais atualizações nem adicionamos aprimoramentos à versão 2020-01-01. Os recursos de UO raiz e UO aninhada não são compatíveis com a versão 2020-01-01.

Propriedades obsoletas na versão do manifesto cFct 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 do cFct

Ao atualizar para a versão 2021-03-15 do esquema de manifesto cFct, 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 de organizações

1. Mova SCPs ou RCPs em 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 UOs deve ser definida na subpropriedade organizational_units. A subpropriedade accounts não é compatível com as políticas da organização.
4. Adicione uma nova propriedade deploy_method com o valor scp ou rcp.

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 deploy_to_ou para a nova propriedade deployment_targets. A lista de UOs deve ser definida na subpropriedade organizational_units.
4. Altere deploy_to_accounts para a nova propriedade deployment_targets. A lista de contas deve ser definida na subpropriedade accounts.
5. Altere a propriedade ssm_parameters para a nova propriedade export_outputs.

Etapas de atualização do cFCT altamente recomendadas

AWS CloudFormation parâmetros

1. Altere a propriedade parameter_file para a nova propriedade parameters.
2. Remova o caminho do arquivo no valor da propriedade parameter_file.
3. Copie a chave e o valor do parâmetro existente do arquivo JSON 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 2021-03-15 do manifesto CFct.

Redes no 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 o AWS Control Tower, consulte Criação de uma infraestrutura de rede multi-VPC AWS escalável e segura.

Tópicos relacionados

- Para obter informações sobre como o AWS Control Tower funciona quando você inscreve contas existentes VPCs, consulteRegistrando contas existentes com VPCs.
- Com o Account Factory, é possível provisionar contas que incluem uma VPC do AWS Control Tower ou provisionar contas sem uma VPC. Consulte informações sobre como excluir a VPC do AWS Control Tower ou configurar contas do AWS Control Tower sem uma VPC em Demonstração: configure o AWS Control Tower sem uma VPC.
- Para obter informações sobre como alterar as configurações da conta 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 na 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 habilitar o controle de negação da região, para que os usuários finais não tenham permissão para se conectar a uma VPC em uma região compatível com o AWS Control Tower, mas fora de suas regiões administradas. Para configurar o controle de negação de região, acesse a página Configurações de zona inicial 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 o AWS padrão VPCs em regiões não governadas. Para listar a VPC padrão em uma região, é possível 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 VPCs

Aqui estão alguns fatos essenciais sobre o AWS Control Tower VPCs:

- 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 do AWS Control Tower pode ter uma VPC criada pelo AWS Control Tower. Uma conta pode ter mais AWS VPCs 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 (N. 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 (N. da Califórnia), cada VPC do AWS Control Tower contém nove sub-redes por padrão, divididas em três zonas de disponibilidade. Na região Oeste dos EUA (N. da Califórnia), seis sub-redes são divididas em duas zonas de disponibilidade.
- Um intervalo exclusivo, de mesmo tamanho é atribuído a cada uma das sub-redes na VPC do AWS Control Tower.
- 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 na 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

> **Gerenciar custos da VPC**
>
> Se você definir a configuração da VPC do Account Factory para que as sub-redes públicas sejam habilitadas ao provisionar uma nova conta, o Account Factory configurará a VPC para criar um gateway NAT. Você será cobrado pelo uso da Amazon VPC.

> **Configurações de VPC e controles**
>
> Se você provisionar contas do Account Factory com as configurações de acesso à internet da VPC habilitadas, essa configuração do Account Factory substituirá o controle Proibir o acesso à internet para uma instância da Amazon VPC gerenciada por um cliente. Para evitar a habilitação do acesso à internet para contas recém-provisionadas, você deve alterar a configuração no Account Factory. Consulte mais informações em Walkthrough: Configure AWS Control Tower Without a 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 o intervalo CIDR geral para a 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 a 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 de até `/16` em 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 desse intervalo)

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`(não IPs fora do `192.168` alcance)

Se o intervalo especificado estiver fora desses, o AWS Control Tower exibirá 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 de cada conta criada dentro da unidade organizacional (UO). Devido à sobreposição padrão de endereços IP, essa implementação não permite inicialmente o emparelhamento entre nenhuma das suas AWS Control Tower VPCs na OU.

Sub-redes

Dentro de cada VPC, o AWS Control Tower divide seu intervalo de CIDR especificado uniformemente em nove sub-redes (exceto no Oeste dos EUA (N. da Califórnia), onde são seis sub-redes). Nenhuma das sub-redes se sobrepõe dentro de uma VPC. Portanto, todas podem se comunicar entre si dentro da VPC.

Em resumo, por padrão, a comunicação de sub-redes 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 VPC-to-VPC peering para comunicação entre vários VPCs. No entanto, por padrão, todas as AWS Control Tower VPCs têm o mesmo intervalo CIDR padrão. Para

permitir o emparelhamento, você pode modificar o intervalo CIDR nas configurações do Account Factory para que os endereços IP não se sobreponham.

Se você alterar o intervalo CIDR nas configurações do Account Factory, todas as novas contas que forem criadas posteriormente pelo AWS Control Tower (usando o Account Factory) receberão o novo intervalo CIDR. As contas antigas não são atualizadas. Por exemplo, você pode criar uma conta, alterar o intervalo de CIDR e criar uma nova conta, e as VPCs alocadas para essas duas contas podem ser pareadas. O emparelhamento é possível porque os intervalos de endereços IP não são idênticos.

Funções e permissões obrigatórias

O AWS Control Tower usa perfis do IAM para ajudar a gerenciar o acesso aos recursos.

Consulte informações sobre perfis em User groups, roles, and permission sets.

Sobre permissões

- Consulte informações sobre grupos do IAM e suas permissões no AWS Control Tower em IAM Identity Center groups for AWS Control Tower.
- Consulte informações sobre as permissões necessárias para provisionar contas em Permissions required for accounts.
- Consulte informações sobre as permissões do console necessárias para o AWS Control Tower em Permissions required to use the AWS Control Tower console.

Sobre perfis

- Consulte informações sobre como criar um perfil, incluindo permissões projetadas para acesso programático em Create roles and assign permissions e em Programmatic roles and trust relationships for the AWS Control Tower audit account.
- Consulte informações sobre outros perfis que o AWS Control Tower usa para gerenciar suas contas em Using identity-based policies (IAM policies) for AWS Control Tower e em Managed policies for AWS Control Tower.
- Para obter informações sobre a AWS Control Tower e as AWS Config funções, consulte AWS Control Tower ConfigRecorderRole.
- Para obter informações sobre as funções que o AWS Control Tower usa para agregar AWS Config informações para suas contas, consulte Como o AWS Control Tower agrega AWS Config regras em contas e não gerenciadas OUs .
- Para obter informações sobre como proteger seus recursos ao atribuir funções e permissões, consulte Condições opcionais para suas relações de confiança de função, Configurar AWS KMS chaves opcionalmente e Evitar a representação entre serviços.
- Consulte informações específicas sobre o provisionamento automatizado de contas no AWS Control Tower com perfis do IAM em Automated Account Provisioning with IAM Roles.
- Para ver a política que protege o tópico do AWS Config SNS, consulte A política do tópico do AWS Config SNS.

Como o AWS Control Tower funciona com perfis para criar e gerenciar contas

Em geral, os perfis fazem parte do Identity and Access Management (IAM) na AWS. Para obter informações gerais sobre o IAM e as funções no AWS, consulte o tópico Funções do IAM no Guia AWS do usuário do IAM.

Criação de conta e perfis

O AWS Control Tower cria uma conta de cliente chamando a API `CreateAccount` do AWS Organizations. Ao AWS Organizations criar essa conta, ela cria uma função dentro dessa conta, que o AWS Control Tower nomeia ao passar um parâmetro para a API. O nome da função é `AWSControlTowerExecution`.

O AWS Control Tower assume o perfil `AWSControlTowerExecution` para todas as contas criadas pelo Account Factory. Usando esse perfil, o AWS Control Tower define a linha de base da conta e aplica controles obrigatórios (e quaisquer outros habilitados), o que resulta na criação de outros perfis. Esses perfis, por sua vez, são usados por outros serviços, como o AWS Config.

> **Note**
>
> Definir a linha de base de conta é configurar seus recursos, que incluem modelos do Account Factory, às vezes chamados de esquemas e controles. O processo de definir a linha de base também configura o registro em log centralizado e os perfis de auditoria de segurança na conta, como parte da implantação dos modelos. As linhas de base do AWS Control Tower estão contidas nos perfis que você aplica a cada conta inscrita.

Consulte mais informações sobre contas e recursos em Sobre Contas da AWS na AWS Control Tower.

O AWSControl TowerExecution papel, explicado

O perfil `AWSControlTowerExecution` deve estar presente em todas as contas inscritas. Ele permite que o AWS Control Tower gerencie suas contas individuais e relate informações sobre elas nas contas de auditoria e de arquivamento de logs.

O perfil `AWSControlTowerExecution` pode ser adicionado a uma conta de várias maneiras, da seguinte forma:

- Para contas na UO de segurança (às vezes chamadas de contas principais), o AWS Control Tower cria o perfil no momento da configuração inicial do AWS Control Tower.
- Para uma conta do Account Factory criada por meio do console do AWS Control Tower, o AWS Control Tower cria esse perfil no momento da criação da conta.
- Para a inscrição de uma única conta, pedimos aos clientes que criem manualmente o perfil e, depois, inscrevam a conta no AWS Control Tower.
- Ao estender a governança para uma OU, o AWS Control Tower usa o StackSet- AWSControl TowerExecutionRole para criar a função em todas as contas dessa OU.

Objetivo do perfil `AWSControlTowerExecution`:

- O `AWSControlTowerExecution` permite criar e inscrever contas, automaticamente, com scripts e funções do 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.
- O `AWSControlTowerExecution` permite que você inscreva uma conta individual no AWS Control Tower. Primeiro, você deve adicionar o perfil `AWSControlTowerExecution` a essa conta. Consulte as etapas sobre como adicionar o perfil em Adicionar manualmente o perfil do IAM necessário a uma Conta da AWS existente e inscrevê-la.

Como a `AWSControlTowerExecution` função funciona com OUs:

O perfil `AWSControlTowerExecution` garante que os controles selecionados do AWS Control Tower se apliquem automaticamente a cada conta individual, em cada UO, na sua organização, bem como a cada nova conta que você criar no AWS Control Tower. Como resultado:

- Você pode fornecer relatórios de conformidade e segurança com mais facilidade, com base nos recursos de auditoria e registro em log incorporados pelos controles do AWS Control Tower.
- Suas equipes de segurança e conformidade podem verificar se todos os requisitos foram atendidos e se houve algum desvio organizacional.

Consulte mais informações sobre desvios em Detect and resolve drift in AWS Control Tower.

Para resumir, a função `AWSControlTowerExecution` e sua política associada fornecem controle flexível de segurança e conformidade em toda a organização. Portanto, as violações de segurança ou protocolo têm menos probabilidade de ocorrer.

Condições opcionais para as relações de confiança do perfil

Você pode impor condições nas políticas de confiança do perfil para restringir as contas e os recursos que interagem com determinados perfis no AWS Control Tower. É altamente recomendável que você restrinja o acesso ao perfil `AWSControlTowerAdmin`, pois ele 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 um `aws:SourceArn` ou `aws:SourceAccount` condicional à instrução da política. Como prática recomendada de segurança, é altamente recomendável adicionar a condição `aws:SourceArn`, porque ela é mais específica do que `aws:SourceAccount`, limitando o acesso a uma conta específica e a um recurso específico.

Se não souber o ARN completo do recurso ou estiver especificando vários recursos, você poderá usar a condição `aws:SourceArn` 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 condição `aws:SourceArn` do IAM com suas políticas de confiança do perfil do IAM. Adicione a condição à sua relação de confiança para a AWSControlTowerAdminfunção, pois o responsável pelo serviço AWS Control Tower interage com ela.

Conforme mostrado no exemplo, o ARN de origem tem o formato: `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Substitua as strings `${HOME_REGION}` e `${CUSTOMER_AWSACCOUNT_id}` 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, o ARN de origem designado como `arn:aws:controltower:us-west-2:012345678901:*` é o único ARN autorizado a realizar a ação `sts:AssumeRole`. Em outras palavras, somente usuários que podem acessar o ID da conta `012345678901`, na região `us-west-2`, podem realizar ações que exijam esse perfil específico e relação de confiança para o serviço AWS Control Tower, designado como`controltower.amazonaws.com`.

O próximo exemplo mostra as condições `aws:SourceAccount` e `aws:SourceArn` aplicadas à política de confiança do perfil.

```
{
  "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 instrução de condição `aws:SourceArn`, com uma instrução de condição `aws:SourceAccount` adicionada. Para obter mais informações, consulte Evitar personificação entre serviços.

Consulte informações gerais sobre políticas de permissão no AWS Control Tower em Gerenciar acesso a recursos.

Recomendações:

Recomendamos que você adicione condições aos perfis que o AWS Control Tower cria, porque esses perfis são assumidos diretamente por outros serviços da AWS. Para obter mais informações, consulte o exemplo de AWSControlTowerAdmin, mostrado anteriormente nesta seção. Para o perfil de gravador do AWS Config , recomendamos adicionar a condição `aws:SourceArn`, especificando o ARN do gravador do Config como o ARN de origem permitido.

Para funções como AWSControlTowerExecutionou outras funções programáticas que podem ser assumidas pela conta de auditoria do AWS Control Tower em todas as contas gerenciadas, recomendamos que você adicione a `aws:PrincipalOrgID` condição à política de confiança dessas funções, o que valida que o principal que acessa o recurso pertence a uma conta na organização correta AWS . Não adicione a instrução da condição `aws:SourceArn`, pois ela não funcionará conforme o esperado.

> **Note**
>
> Em caso de desvio, é possível que um perfil do AWS Control Tower seja redefinido em determinadas circunstâncias. É recomendável que você verifique novamente os perfis periodicamente, caso os tenha personalizado.

Como o AWS Control Tower agrega AWS Config regras em contas e não gerenciadas OUs

A conta de gerenciamento da AWS Control Tower cria um agregador em nível organizacional, que ajuda na detecção de AWS Config regras externas, para que a AWS Control Tower não precise obter acesso a contas não gerenciadas. O console do AWS Control Tower mostra quantas AWS Config regras criadas externamente você tem para uma determinada conta. Consulte detalhes sobre essas regras externas na guia Conformidade de regras externas do Config da página de Detalhes da conta.

Para criar o agregador, o AWS Control Tower adiciona um perfil com as permissões necessárias para descrever uma organização e listar as contas que ela contém. O perfil `AWSControlTowerConfigAggregatorRoleForOrganizations` requer a política gerenciada `AWSConfigRoleForOrganizations` e uma relação de confiança com `config.amazonaws.com`.

Aqui está a política do IAM (artefato JSON) anexada ao perfil:

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

Esta é a relação de confiança de `AWSControlTowerConfigAggregatorRoleForOrganizations`:

```
{
    "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 tudo pronto, você poderá inscrever contas individualmente ou inscrevê-las como um grupo registrando uma UO. Quando você inscreve uma conta, se você cria uma regra no AWS Config, o 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 console do AWS Config e no console do AWS Control Tower para determinar se você tem os controles apropriados habilitados para a conta.

Perfis programáticos e relações de confiança para a conta de auditoria do AWS Control Tower

É possível entrar na conta de auditoria e assumir o perfil 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 que são concedidas somente às funções do AWS Lambda. Para fins de segurança, esses perfis têm relações de confiança com outros perfis, o que significa que as condições sob as quais os perfis podem ser utilizados são estritamente definidas.

A pilha `StackSet-AWSControlTowerBP-BASELINE-ROLES` do AWS Control Tower cria esses perfis do IAM somente programáticos e entre contas na conta de auditoria:

- aws-control tower- AdministratorExecutionRole
- aws-control tower- ReadOnlyExecutionRole

A pilha `StackSet-AWSControlTowerSecurityResources` do AWS Control Tower cria esses perfis do IAM somente programáticos e entre contas na conta de auditoria:

- aws-control tower- AuditAdministratorRole
- aws-control tower- AuditReadOnlyRole

`ReadOnlyExecutionRole:` Observe que esse perfil permite que a conta de auditoria leia objetos nos buckets do Amazon S3 em toda a organização (em contraste com a política `SecurityAudit`, que permite somente o acesso aos metadados).

aws-control tower-: AdministratorExecutionRole

- Tem permissões de administrador
- Não pode ser assumido pelo console
- Só pode ser assumido por um perfil na conta de auditoria: o `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 número `Audit_acct_ID` 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 somente pelo AWS serviço Lambda
- Tem permissão para realizar operações de leitura (Get) e gravação (Put) em objetos do Amazon S3 com nomes que começam com o log da string

Políticas anexadas:

1. AWSLambdaExecutar — política AWS gerenciada

2. AssumeRole-aws-controltower- AuditAdministratorRole — política em linha — Criada pela AWS Control Tower, 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 de `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 pelo console
- Só pode ser assumido por outro perfil na conta de auditoria: o `AuditReadOnlyRole`

O artefato a seguir mostra a relação de confiança de `aws-controltower-ReadOnlyExecutionRole`. O número do espaço reservado `012345678901` será substituído pelo número `Audit_acct_ID` 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 somente pelo AWS serviço Lambda
- Tem permissão para realizar operações de leitura (Get) e gravação (Put) em objetos do Amazon S3 com nomes que começam com o log da string

Políticas anexadas:

1. AWSLambdaExecutar — política AWS gerenciada

2. AssumeRole-aws-controltower- AuditReadOnlyRole — política em linha — Criada pela AWS Control Tower, 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 de `aws-controltower-AuditAdministratorRole`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Provisionamento automatizado de conta com funções do IAM

Para configurar 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. Depois, usando o perfil, a conta de gerenciamento executa as etapas de configuração desejadas em cada conta-membro.

Se você estiver provisionando contas usando funções do Lambda, a identidade que executará esse trabalho deverá ter a política de permissões do IAM a seguir, 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: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 pelo AWS Control Tower Account Factory para interagir com o AWS IAM Identity Center.

Recursos no AWS Control Tower

- Consulte informações gerais sobre a propriedade de recursos no AWS Control Tower em Visão geral do gerenciamento de permissões de acesso aos recursos do AWS Control Tower.
- Consulte informações sobre os recursos que o AWS Control Tower cria nas contas compartilhadas em Sobre as contas compartilhadas.
- Consulte informações sobre os recursos que o AWS Control Tower cria ao provisionar uma conta por meio do Account Factory em Considerações 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 do AWS Control Tower no Guia AWS CloudFormation do usuário.

Como AWS as regiões funcionam com o AWS Control Tower

Atualmente, o AWS 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 (Norte da Califórnia)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Jacarta)
- Ásia Pacifico (Osaka)
- Europa (Milão)
- África (Cidade do Cabo)
- Oriente Médio (Bahrein)
- Israel (Tel Aviv)
- Oriente Médio (Emirados Árabes Unidos)

- Europa (Espanha)
- Ásia-Pacífico (Hyderabad)
- Europa (Zurique)
- Ásia-Pacífico (Melbourne)
- Oeste do Canadá (Calgary)
- Malásia (Kuala Lumpur)

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 escolher uma região de origem, não é possível alterá-la.

Controles e regiões

No momento, todos os controles preventivos funcionam globalmente. No entanto, controles detectivos e proativos só funcionam em regiões nas quais o AWS Control Tower é compatível. Consulte mais informações sobre o comportamento de controles ao ativar o AWS Control Tower em uma nova região em Configurar regiões do AWS Control Tower.

Configurar regiões do AWS Control Tower

Esta seção descreve o comportamento que você pode esperar ao estender sua zona de pouso do 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 Atualizar do console do AWS Control Tower.

> **Note**
>
> Recomendamos que você evite expandir a zona de pouso do AWS Control Tower para regiões da AWS nas quais as workloads não precisam ser executadas. O cancelamento de uma região não impede que você implante recursos nela, mas eles permanecerão fora da governança do AWS Control Tower.

Durante a configuração de uma nova região, o AWS Control Tower atualiza a zona de pouso, o que significa que ele define como linha de base a sua zona de pouso.

- para operar ativamente em todas as regiões recém-selecionadas, e
- para deixar de administrar recursos em regiões não selecionadas.

As contas individuais dentro de suas unidades organizacionais (OUs) que são gerenciadas pelo 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 as regiões do AWS Control Tower, preste atenção a estas recomendações e limitações:

- Selecione regiões nas quais você planeja hospedar AWS recursos ou cargas de trabalho.
- O cancelamento de uma região não impede que você implante recursos nela, mas eles permanecerão fora da governança do AWS Control Tower.

Ao configurar a zona de pouso para novas regiões, os controles de detecção do 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 do AWS Control Tower em uma nova região (atualizando sua zona de pouso), você deve atualizar as contas existentes na sua atual OUs antes de poder habilitar novos controles de detetive sobre essas OUs e suas contas.
- Os controles de detecção existentes começam a funcionar nas regiões recém-configuradas assim que as contas são atualizadas. Ao atualizar a zona de pouso do AWS Control Tower para configurar novas regiões e, então, atualizar uma conta, os controles de detecção que já estão habilitados na UO começarão a funcionar nessa conta nas regiões recém-configuradas.

Configurar regiões do AWS 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, selecione Configurações de zona inicial.

3. Na página Configurações de zona inicial, na seção Detalhes, escolha o botão Modificar configurações no canto superior direito. Isso redireciona ao fluxo de trabalho de atualização da zona de pouso, porque administrar novas regiões ou remover regiões da governança exige uma atualização 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 administra atualmente e quais não.
5. Marque a caixa de seleção para cada região adicional a ser administrada. Desmarque a caixa de seleção de cada região da qual você está removendo a governança.

   > **Note**
   >
   > Se você optar por não administrar uma região, ainda poderá implantar recursos nela, mas eles permanecerão fora da governança do AWS Control Tower.

6. Conclua o restante do fluxo de trabalho e selecione Atualizar zona de pouso.
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 depois de configurar novas regiões é usando o framework de API do Service Catalog e a AWS CLI para atualizar as contas em um processo em lote. Para obter mais informações, consulte Provisionar e atualizar contas usando automação.

Evitar 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 poderá ocorrer se os controles que regem uma UO não corresponderem totalmente aos controles que administrar cada conta dentro de uma UO. A governança mista ocorre em uma OU se as contas não forem atualizadas depois que o AWS Control Tower estender a governança para uma nova Região da AWS ou remover a governança.

Nessa situação, determinadas contas em uma UO podem ter controles diferentes aplicados em diferentes regiões, quando comparadas a outras contas na UO ou quando comparadas ao procedimento geral de governança da zona de pouso.

Em uma UO com governança mista, se você provisionar uma nova conta, ela receberá o mesmo (atualizado) procedimento de governança da região e da UO que a zona de pouso. No entanto, as contas existentes que ainda não foram atualizadas não recebem o procedimento atualizado 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 registradas OUs, para contas que ainda não foram atualizadas.

> **Note**
>
> O AWS Control Tower não permite que controles sejam habilitados durante um estado de governança mista.

Comportamento dos controles durante a governança mista

- Durante a governança mista, o 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 de erro `FAILED_TO_ENABLE`.
- Durante a governança mista, se você estender a governança da zona de pouso para uma região opcional enquanto nenhuma conta na UO ainda não tiver sido atualizada, a operação da API `EnableControl` na UO falhará nos controles proativos e de detecção. Você receberá uma mensagem de erro `FAILED_TO_ENABLE`, pois contas-membros não atualizadas dentro da UO ainda não foram incluídas nessas regiões.
- Durante a governança mista, controles que fazem parte do Padrão gerenciado pelo serviço Security Hub: AWS Control Tower não podem relatar a conformidade com precisão em regiões onde há uma incompatibilidade entre a configuração da zona de pouso e as contas que não estão atualizadas.
- A governança mista não altera o comportamento dos controles baseados em SCP (controles preventivos), que se aplicam uniformemente a todas as contas em uma UO, em todas as regiões governadas.

> **Note**
>
> Governança mista não é o mesmo que desvio e não é relatada como desvio.

Como reparar a governança mista

- Escolha Atualizar conta para cada conta na UO que mostre o status Atualização disponível na página Organizações 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 como ativar as regiões opcionais da 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 opcional tem uma base histórica. As Regiões da AWS introduzidas após 20 de março de 2019 são consideradas regiões opcionais. As regiões opcionais têm requisitos de segurança mais altos do que as regiões comerciais, no que diz respeito ao compartilhamento de dados do IAM por meio de contas ativas nas regiões opcionais. Todos os dados gerenciados por meio do serviço IAM são considerados dados de identidade, incluindo usuários, grupos, perfis, políticas, provedores de identidade, os 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.

É possível ativar regiões opcionais automaticamente durante a configuração da zona de pouso, selecionando-as. A zona de pouso 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 Habilitar uma região, quando estiver conectado ao AWS Management Console. Para trazer suas próprias contas existentes de auditoria e de arquivamento de logs 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 Europa (Milão), eu-south-1
- Região África (Cidade do Cabo), af-south-1
- Região Oriente Médio (Bahrein), me-south-1
- Israel (Tel Aviv), il-central-1
- Região Oriente Médio (EAU), me-central-1
- Região Europa (Espanha), eu-south-2
- Região Ásia-Pacífico (Hyderabad), ap-south-2
- Região Europa (Zurique), eu-central-2
- Região Ásia-Pacífico (Melbourne), ap-southeast-4
- Região Oeste do Canadá (Calgary), ca-west-1

O AWS 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 workloads em regiões opcionais.

> **Governar ou ativar?**
>
> 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 à região. Ativar ou desativar uma região opcional é uma ação diferente que você pode escolher no console da AWS , que abre a região em sua conta, para que você possa implantar recursos e workloads na região.

Considerações comportamentais

- Se você decidir governar regiões opcionais, recomendamos que não desative (cancele) nenhuma das regiões opcionais governadas, pois isso pode causar falha nas suas workloads. O AWS Control Tower não permite a desativação de uma região governada de dentro do console da AWS Control Tower, mas certifique-se de não desativar regiões governadas de uma fonte fora da AWS Control Tower, como o console de AWS faturamento ou o SDK. AWS

- Quando o AWS Control Tower estende a governança para uma região opcional, ele ativa (aceita) a região em todas as contas-membros. Quando você remove uma região da governança, o AWS Control Tower não desativa (cancela) a região nas contas-membros.
- Durante a desseleção da região, o 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 AWS Control Tower, como o console de AWS faturamento ou o SDK. AWS Recomendamos que você remova recursos das regiões que desativou ou poderá receber cobranças inesperadas por esses recursos.
- Se a zona de pouso for desativada, o AWS Control Tower limpará os recursos em todas as regiões governadas, incluindo as regiões opcionais. No entanto, o AWS Control Tower não desativa as regiões opcionais. É possível desativar as regiões opcionais como uma etapa adicional após a desativação.
- Se a região de origem for uma região opcional e se você pretende inscrever contas existentes como contas de auditoria e arquivamento de logs, ative manualmente a região opcional antes de selecioná-la como a região de origem da zona de pouso. Consulte Enabling a Region.
- Se o AWS Control Tower estiver configurado 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.
- A API subjacente 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 administradas, incluindo regiões opcionais, o limite máximo do número de contas por unidade organizacional (UO) será reduzido ao registrar uma UO. Para obter mais informações, consulte Limitações com base nos AWS serviços subjacentes.

Configurar o controle de negação de região

O AWS Control Tower oferece dois controles de negação de região. Um controle, `GRREGIONDENY`, que quando ativado, se aplica a toda a zona de pouso. 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 o controle de negação de região da zona de pouso

O controle de negação de região, `GRREGIONDENY` é único, pois se aplica à zona de pouso como um todo, e não a uma UO específica. Para configurar o controle de negação de região, acesse a página Configurações de zona inicial e selecione Modificar configurações.

- Essa configuração pode ser alterada posteriormente.
- Quando ativado, esse controle se aplica a todos os cadastrados OUs.
- Esse controle não pode ser configurado individualmente OUs.

> **Note**
>
> Antes de habilitar o controle de negação de região, verifique se não há recursos nessas regiões, pois você não terá acesso a eles depois de aplicar o controle. Enquanto o controle estiver habilitado, 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 governadas na AWS Control Tower que permanecem com o status Não governado, e você pode implantar recursos em regiões fora da disponibilidade do AWS Control Tower.

> **Exceções**
>
> Você não pode negar o acesso à região de origem. Certos AWS serviços globais, como IAM e AWS Organizations, estão isentos do controle de negação da região. Para saber mais, consulte Deny access to AWS based on the requested 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.
- Esse é um controle eletivo com orientação preventiva.

Consulte o modelo de SCP do controle de negação de região em Deny access to AWS based on the requested Região da AWS na Referência de controles do AWS Control Tower. O AWS Control Tower SCP é semelhante ao SCP AWS Organizations, mas não idêntico.

É possível determinar os endpoints do serviço regional na página Serviços regionais.

Considerações sobre o controle de negação de região no nível da UO

A principal consideração sobre o controle de negação de região no nível da UO é determinar como ele interagirá com o controle de negação de região da zona de pouso, se ambos estiverem ativados. Consulte mais informações em Region deny control applied to the OU.

Talvez você também queira consultar Configure the Region deny control.

Provisionar e gerenciar contas no AWS Control Tower

Este capítulo inclui uma visão geral e procedimentos para provisionar e gerenciar contas-membros na zona de pouso do AWS Control Tower.

Também inclui uma visão geral e procedimentos para inscrever uma AWS conta existente no AWS Control Tower.

Consulte mais informações sobre contas no AWS Control Tower em Sobre Contas da AWS na AWS Control Tower. Consulte informações sobre a inscrição de várias contas no AWS Control Tower em Registrar uma unidade organizacional existente com o AWS Control Tower.

> **Note**
>
> É possível realizar até cinco (5) operações relacionadas a contas simultaneamente, incluindo provisionamento, atualização e inscrição.

Métodos de provisionamento

O AWS Control Tower fornece vários métodos para criar e atualizar contas-membros. Alguns métodos são baseados fundamentalmente no console e outros são principalmente automatizados.

Visão geral

A forma padrão de criar contas-membros é por meio do Account Factory, um produto baseado em console que faz parte do Service Catalog. Se a zona de pouso não estiver em um estado de desvio, você poderá usar Criar conta como um método para adicionar novas contas do console, bem como Inscrever conta para inscrever contas da AWS existentes no AWS Control Tower.

Com o Account Factory, é possível provisionar contas básicas, contando com as configurações padrão do 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 pelo console do AWS Control Tower. Além disso, ele automatiza a personalização e a implantação de contas. Ele permite o provisionamento automatizado baseado no console, após algumas etapas únicas de configuração, o que elimina a necessidade de escrever scripts ou configurar pipelines. Consulte mais informações em Personalizar contas com Account Factory Customization (AFC).

Métodos baseados no console:

- Por meio do console Account Factory que faz parte do AWS Service Catalog, para contas básicas ou personalizadas. Consulte detalhes e instruções em Provisione e gerencie contas com o Account Factory.
- Por meio do recurso Inscrever conta no AWS Control Tower, se a zona de pouso não estiver em um estado de desvio. Consulte Inscrever uma conta existente.
- No console do AWS Control Tower, é possível usar o Account Factory para criar, atualizar ou inscrever até cinco contas ao mesmo tempo.

Métodos automatizados:

- Código do Lambda: da sua conta de gerenciamento da zona de pouso do AWS Control Tower, usando o código do Lambda e os perfis do IAM apropriados. Consulte Automated Account Provisioning with IAM Roles.
- Terraform: do AWS Control Tower Account Factory for Terraform (AFT), que depende do Account Factory e de um GitOps modelo para permitir a automação do provisionamento e da atualização de contas. Consulte Provisionar contas com o Account Factory for Terraform (AFT) do AWS Control Tower .
- Account Factory Customization no console do AWS Control Tower: após as etapas de configuração, o provisionamento futuro de contas personalizadas não exige 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 esquemas do Terraform podem implantar recursos somente em uma única região. Por padrão, é a região de origem.

O que acontece quando o 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 ver as etapas para

cadastrar um existente Conta da AWS usando o console do 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 a `ProvisionProduct` API Service Catalog.
2. AWS Service Catalog chama o AWS Control Tower.
3. O AWS Control Tower inicia um fluxo de trabalho que, como primeira etapa, chama a AWS Organizations `CreateAccount` API.
4. Depois de AWS Organizations criar a conta, o AWS Control Tower conclui o processo de provisionamento aplicando esquemas e controles.
5. O Service Catalog continua a inspecionar o AWS Control Tower para verificar a conclusão do processo de provisionamento.
6. Quando o fluxo de trabalho no AWS Control Tower é concluído, o Service Catalog finaliza o estado da conta e informa você (o solicitante) sobre o resultado.

Permissões obrigatórias para contas

As permissões obrigatórias para cada método de provisionamento e atualização de contas são discutidas em cada seção, respectivamente. Com as permissões do grupo de usuários apropriado, os provisionadores podem especificar linhas de base padronizadas e configurações de rede para todas as contas na organização.

> **Note**
>
> Ao provisionar uma conta, o solicitante da conta sempre deve ter as permissões `CreateAccount` e `DescribeCreateAccountStatus`. Esse conjunto de permissões faz parte do perfil de Administrador e é concedido automaticamente quando um solicitante assume esse perfil. Se você delegar permissão para provisionar contas, talvez seja necessário adicionar essas permissões diretamente aos solicitantes da conta.

Ao criar contas no console do AWS Control Tower com o Account Factory, é necessário se conectar a uma conta com um usuário do IAM que tenha a política

`AWSServiceCatalogEndUserFullAccess` habilitada, junto com permissões para usar o console do AWS Control Tower, e você não pode se conectar como usuário-raiz.

Consulte informações gerais sobre as permissões exigidas no AWS Control Tower em Uso de políticas baseadas em identidade (políticas do IAM) para o AWS Control Tower. Consulte informações sobre perfis e contas no AWS Control Tower em Roles and accounts.

> **Segurança para contas**
>
> É possível encontrar orientações sobre as práticas recomendadas para proteger a segurança da conta de gerenciamento do AWS Control Tower e das contas-membros na documentação do AWS Organizations .
>
> - Best practices for the management account
> - Best practices for member accounts

Sobre Contas da AWS na AWS Control Tower

An Conta da AWS é o contêiner para todos os seus recursos próprios. Esses recursos incluem as identidades AWS Identity and Access Management (IAM) aceitas pela conta, que determinam quem tem acesso a essa conta. As identidades do IAM podem incluir usuários, grupos, perfis e muito mais. Consulte mais informações sobre como trabalhar com perfis, políticas e usuários do IAM no AWS Control Tower em Identity and access management in AWS Control Tower.

Recursos e tempo de criação da conta

Quando o AWS Control Tower cria ou inscreve uma conta, ele implanta a configuração mínima necessária de recursos para a conta, incluindo recursos na forma de modelos do Account Factory e outros recursos na zona de pouso. Esses recursos podem incluir funções do IAM, AWS CloudTrail trilhas, produtos provisionados pelo Service Catalog e usuários do IAM Identity Center. O AWS Control Tower também implanta recursos, conforme exigido pela configuração de controle, para a unidade organizacional (UO) na qual a nova conta está destinada a se tornar uma conta-membro.

O AWS 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. Consulte mais informações sobre como gerenciar recursos nas contas em Orientações para criar e modificar recursos do AWS Control Tower.

Considerações sobre como trazer contas de segurança ou registro em log existentes

Antes de aceitar uma conta Conta da AWS como de segurança ou de registro, a AWS Control Tower verifica a conta em busca de recursos que estejam em conflito com os requisitos da AWS Control Tower. Por exemplo, é possível ter um bucket de registro em log com o mesmo nome exigido pelo AWS Control Tower. Além disso, o 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.

O AWS Control Tower não remove nenhum recurso existente nas contas de registro em log 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.

Visualizar contas

A página Organização lista todas OUs as contas da sua organização, independentemente da OU ou do status de inscrição no AWS Control Tower. É possível visualizar e inscrever contas-membros no AWS Control Tower, individualmente ou por grupos de UO, se cada conta atender aos pré-requisitos de inscrição.

Para ver uma conta específica na página Organização, é possível escolher Somente contas no menu suspenso no canto superior direito e, depois, selecionar o nome da conta na tabela. Como alternativa, é possível selecionar o nome da UO principal na tabela e exibir uma lista de todas as contas dessa UO na página Detalhes dessa UO.

Na página Organização e na página Detalhes da conta, é possível ver o Estado da conta, que é um destes:

- Não cadastrada: a conta é membro da UO principal, mas não é totalmente gerenciada pelo AWS Control Tower. Se a UO principal estiver registrada, a conta será administrada pelos controles preventivos configurados para sua UO principal registrada, mas os controles de detecção da UO não se aplicam a essa conta. Se a UO principal não estiver registrada, nenhum controle se aplicará a essa conta.
- Inscrevendo: a conta está sendo incorporada à governança pelo AWS Control Tower. Estamos alinhando a conta com a configuração de controle da UO principal. Esse processo pode exigir vários minutos por recurso da conta.

- Inscrita: a conta é administrada pelos controles configurados para a UO principal. Ela é totalmente administrada pelo AWS Control Tower.
- Falha na inscrição: não foi possível inscrever a conta no AWS Control Tower. Para obter mais informações, consulte Causas comuns para falha de 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 no ambiente. Para atualizar uma única conta, acesse a página de detalhes da conta e selecione Atualizar conta.

  Se você tiver várias contas com esse estado em uma única UO, poderá optar por Registrar novamente a UO e atualizar essas contas em conjunto.

Recursos criados nas contas compartilhadas

Esta seção mostra os recursos que o AWS Control Tower cria nas contas compartilhadas quando você configura a zona de pouso.

Consulte informações sobre os recursos de conta-membro em Considerações 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.

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS Organizations	Contas	audit log archive
AWS Organizations	OUs	Security Sandbox
AWS Organizations	Políticas de controle de serviço	aws-guardrails-*

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS CloudFormation	Pilhas	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER (na versão 2.6 e posterior)

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL (Não implantado na versão 3.0 e versões posteriores) AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED AWSControlTowerLoggingResources

Serviço da AWS	Tipo de recurso	Nome do recurso
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Produto	Account Factory do AWS Control Tower
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	Perfis	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Políticas	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS IAM Identity Center	Grupos de diretórios	AWSAccountFábrica AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	Conjuntos de permissões	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess 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 a atualize.

Recursos da conta de arquivamento de logs

Quando você configura sua landing zone, os seguintes AWS recursos são criados em sua conta de arquivamento de registros.

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS CloudFormation	Pilhas	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

Serviço da AWS	Tipo de recurso	Nome do recurso
		StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	Regras do AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED 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

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS Identity and Access Management	Perfis	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole 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-* 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.

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS CloudFormation	Pilhas	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

Serviço da AWS	Tipo de recurso	Nome do recurso
		StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*
AWS Config	Agregador	aws-controltower-GuardrailsComplianceAggregator
AWS Config	Regras do AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED 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

Serviço da AWS	Tipo de recurso	Nome do recurso
AWS Identity and Access Management	Perfis	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	Políticas	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Tópicos	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications 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.

- É possível escolher nomes personalizados para as contas de auditoria e de arquivo de logs ao configurar a zona de pouso. Consulte informações sobre como alterar o nome de uma conta em Externally changing AWS Control Tower resource names.
- Você também pode especificar uma conta existente Conta da AWS como segurança ou de registro do AWS Control Tower durante o processo inicial de configuração da landing zone. Essa opção elimina a necessidade de o AWS Control Tower criar contas novas e compartilhadas. (Essa é uma seleção única.)

Consulte mais informações sobre contas compartilhadas e seus recursos associados em Recursos criados nas contas compartilhadas.

Conta de gerenciamento

Isso Conta da AWS lança o AWS Control Tower. Por padrão, o usuário-raiz dessa conta e o usuário do IAM ou usuário administrador do IAM dessa conta têm acesso total a todos os recursos na zona de pouso.

> **Note**
>
> Como prática recomendada, aconselhamos fazer login como usuário do Centro de identidade do IAM com privilégios de Administrador ao realizar funções administrativas no console do AWS Control Tower, em vez de fazer login como usuário-raiz ou usuário administrador do IAM dessa conta.

Consulte mais informações sobre os perfis e os recursos disponíveis na conta de gerenciamento em Recursos criados nas contas compartilhadas.

Conta de arquivamento de logs

A conta compartilhada de arquivamento de logs é configurada automaticamente quando você cria a zona de pouso.

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, aconselhamos restringir o acesso à conta de arquivamento de logs 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 zona de pouso do AWS Control Tower versão 3.3 e posterior, as contas devem atender a uma condição `aws:SourceOrgID` para qualquer permissão de gravação no 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 S3 do AWS Control Tower. Para obter mais informações, consulte Versão 3.3 da zona de pouso do AWS Control Tower.

Consulte mais informações sobre os perfis e os recursos disponíveis na conta de arquivamento de logs em Recursos da conta de arquivamento de logs.

> **Note**
>
> Esses logs não podem ser alterados. Todos os logs 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 a zona de pouso.

A conta de auditoria deve ser restrita às equipes de segurança e conformidade com perfis entre contas de auditor (somente leitura) e administrador (acesso total) em todas as contas na zona de pouso. Esses perfis devem ser usados pelas equipes de segurança e conformidade para:

- Realize auditorias por meio de AWS mecanismos, como hospedar funções Lambda de AWS Config regras personalizadas.
- Executar operações de segurança automatizadas, como ações de correção.

A conta de auditoria também recebe notificações por meio do serviço Amazon Simple Notification Service (Amazon SNS). 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 contas OUs, usuários e em sua SCPs landing zone. Consulte mais informações sobre o desvio em Detectar e resolver desvios no AWS Control Tower.

As notificações de auditoria que são acionadas em uma conta-membro também podem enviar alertas para um tópico local do Amazon SNS. Essa funcionalidade permite que os administradores da conta assinem notificações de auditoria específicas de uma conta-membro individual. Como resultado, os administradores podem resolver problemas que afetam uma conta individual e, ao mesmo tempo, agregar todas as notificações da conta na conta de auditoria centralizada. Consulte mais informações no Guia do desenvolvedor do Amazon Simple Notification Service.

Consulte mais informações sobre os perfis e os recursos disponíveis na conta de auditoria em Recursos da conta de auditoria.

Consulte mais informações sobre a auditoria programática em Programmatic roles and trust relationships for the AWS Control Tower audit account.

> **Important**
>
> O endereço de e-mail fornecido para a conta de auditoria receberá e-mails de Notificação da AWS : confirmação da assinatura de cada Região da AWS compatível com o 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 pelo AWS Control Tower.

Sobre contas-membros

As contas de membros são as contas por meio das quais seus usuários realizam suas AWS cargas de trabalho. Essas contas-membros podem ser criadas no Account Factory, por usuários do Centro

de Identidade do IAM com privilégios de Administrador no console do Service Catalog ou por métodos automatizados. Quando criadas, essas contas-membros existem em uma UO que foi criada no console do AWS Control Tower ou registrada com o AWS Control Tower. Consulte mais informações nestes tópicos relacionados:

- Provisione e gerencie contas com o Account Factory
- Automatizar tarefas no AWS Control Tower
- AWS Organizations Terminology and Concepts no Guia do usuário do AWS Organizations .

Também consulte Provisionar contas com o Account Factory for Terraform (AFT) do AWS Control Tower .

> **Contas e controles**
>
> As contas-membros podem ser inscritas no AWS Control Tower ou podem ser não inscritas. 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 herança OUs .

Consulte informações sobre os recursos da conta-membro que o AWS Control Tower aloca em Considerações sobre recursos do Account Factory.

Inscrever um existente Conta da AWS

Você pode estender a governança da AWS Control Tower para 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 qualificadas em pessoas não registradas OUs que fazem parte da mesma AWS Organizations organização da OU do AWS Control Tower.

> **Note**
>
> Você não pode inscrever uma conta existente para servir como sua conta de auditoria ou arquivamento de logs, exceto durante a configuração inicial da zona de pouso.

Configurar primeiro o acesso confiável

Antes de inscrever um existente Conta da AWS no AWS Control Tower, você deve dar permissão para que o AWS Control Tower gerencie ou controle a conta. Especificamente, o AWS Control Tower exige permissão para estabelecer um acesso confiável entre AWS CloudFormation e AWS Organizations em seu nome, para que AWS CloudFormation você possa implantar sua pilha automaticamente nas contas da organização selecionada. Com esse acesso confiável, o perfil `AWSControlTowerExecution` realiza as atividades necessárias para gerenciar cada conta. É por isso que você deve adicionar esse perfil 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. O AWS Control Tower depende dessa capacidade de confiança para poder aplicar perfis e permissões às contas existentes antes de transferi-las a uma unidade organizacional registrada e, assim, colocá-las sob governança.

Para saber mais sobre acesso confiável e AWS CloudFormation StackSets, veja AWS CloudFormationStackSetsAWS Organizationse.

O que acontece durante a inscrição da conta

Durante o processo de inscrição, o AWS Control Tower executa estas 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 do 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, ela é administrada pela trilha do AWS CloudTrail 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 no AWS Control Tower.
> - Se você mover uma conta para uma UO registrada, por exemplo, por meio do console do AWS Organizations , e não continuar a inscrever a conta no AWS Control Tower, 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

O AWS 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 a VPC AWS padrão e cria uma nova VPC para essa conta.
- Quando você registra uma conta existente, o AWS Control Tower não cria uma VPC para essa conta.
- Quando você inscreve uma conta existente, o AWS Control Tower não remove nenhuma VPC existente nem VPC padrão da AWS associada à conta.

> **Tip**
>
> É possível alterar o comportamento padrão de novas contas configurando o Account Factory, para que uma VPC não seja configurada por padrão para contas na organização no AWS Control Tower. Para obter mais informações, consulte Criar uma conta no AWS Control Tower sem uma VPC.

Pré-requisitos da inscrição

Esses pré-requisitos são necessários antes que você possa inscrever um existente no AWS Control Conta da AWS Tower:

1. Para cadastrar uma existente Conta da AWS, a `AWSControlTowerExecution` função deve estar presente na conta que você está cadastrando. Você pode consultar detalhes e instruções em Enroll an account.
2. Além do perfil `AWSControlTowerExecution`, a Conta da AWS existente 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 pela AWS CLI antes que você possa inscrever

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 organização do AWS Organizations como a conta de gerenciamento do AWS Control Tower. A conta que existe podem ser inscritas apenas na mesma organização da conta de gerenciamento do AWS Control Tower, em uma UO que já esteja registrada no AWS Control Tower.

Consulte outros pré-requisitos de inscrição em Getting Started with AWS Control Tower.

> **Note**
>
> Quando você inscreve uma conta no AWS Control Tower, ela é administrada pela trilha do AWS CloudTrail da organização do 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 no AWS Control Tower.

Inscrever uma conta existente

O recurso de inscrição de contas está disponível no console do AWS Control Tower, para cadastrar contas existentes, de Contas da AWS forma que sejam governadas pela AWS Control Tower. Para obter mais informações, consulte Inscrever um existente Conta da AWS.

O recurso Inscrever conta estará disponível quando a zona de pouso não estiver em um estado de desvio. Como visualizar esse recurso no console:

- Acesse a página Organização no AWS Control Tower.
- Encontre o nome da conta que você deseja inscrever. 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 inscrever uma conta individual, conforme mostrado na seção Etapas para inscrever uma conta.

> **Note**
>
> Ao inscrever um existente Conta da AWS, certifique-se de verificar o endereço de e-mail existente. Caso contrário, uma 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. Será necessário provisionar novas contas por meio do Account Factory até que o desvio da zona de pouso seja resolvido.

Ao inscrever contas pelo console do AWS Control Tower, é necessário fazer login em uma conta com um usuário do IAM que tenha a política `AWSServiceCatalogEndUserFullAccess` habilitada, junto com permissões de acesso de administrador para usar o console do AWS Control Tower, e você não pode se conectar como usuário-raiz.

As contas que você cadastrar podem ser atualizadas por meio da AWS Service Catalog fábrica de contas do 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 inscrever uma conta

Depois que a AdministratorAccesspermissão (política) estiver em vigor em sua conta existente, siga estas etapas para registrar a conta:

Como inscrever uma conta individual no AWS Control Tower

- Acesse a página Organização do AWS Control Tower.
- Na página Organização, as contas que elegíveis para inscrição permitem que você selecione Inscrever no menu suspenso Ações na parte superior da seção. Essas contas também mostram um botão Inscrever conta quando você as visualiza na página Detalhes da conta.
- Ao escolher Inscrever conta, você verá uma página Inscrever conta, na qual será solicitado que você adicione o perfil `AWSControlTowerExecution` à conta. Consulte instruções em Adicionar manualmente o perfil do IAM necessário a uma Conta da AWS existente e inscrevê-la.
- Depois, selecione uma UO registrada na lista suspensa. Se a conta já estiver em uma UO registrada, essa lista mostrará a UO.
- Escolha Enroll account (Registrar conta).
- Você verá um lembrete modal para adicionar o perfil `AWSControlTowerExecution` e confirmar a ação.
- Escolha Inscrever.
- O AWS Control Tower inicia o processo de inscrição e você é direcionado de volta à página Detalhes da conta.

Causas comuns para falha de inscrição

- Para inscrever uma conta existente, o perfil `AWSControlTowerExecution` deve estar presente na conta que você está inscrevendo.
- Sua entidade principal do IAM 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 pelo AWS Control Tower.
- Você pode ter feito login com uma conta que precisa ser adicionada ao portfólio do Account Factory no AWS Service Catalog. A conta deve ser adicionada antes que você tenha acesso ao Account Factory para que seja possível criar ou inscrever uma conta no AWS Control Tower. Se o usuário ou perfil apropriado não for adicionado ao portfólio do Account Factory, será exibido um 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 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 do AWS Config existentes e Interaja com AWS Control Tower por meio de AWS CloudShell.
- Se a conta pertencer a outra UO com uma conta de gerenciamento, incluindo outra UO do AWS Control Tower, você deverá encerrar a conta em sua UO atual antes que ela possa ingressar em outra UO. Os recursos existentes devem ser removidos na UO 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 SCP na UO de destino pode bloquear a criação de recursos sem determinadas tags. Nesse caso, o provisionamento ou a inscrição da conta falham, porque o AWS Control Tower não permite a marcação de recursos. Se precisar de ajuda, entre em contato com seu representante de conta ou com o Suporte.

Consulte mais informações sobre como o AWS Control Tower funciona com perfis quando você está criando contas ou registrando contas existentes em Roles and accounts.

> **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 UO desejada. Se a inscrição falhar, nenhuma outra conta ou OUs será afetada pela falha.

Se tiver dúvidas de que suas contas existentes e suas configurações são compatíveis com o AWS Control Tower, você poderá seguir as práticas recomendadas indicadas 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 controles do AWS 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 do AWS Control Tower, talvez seja necessário remover o canal de AWS Config entrega e o gravador de configuração que foram criados para sua avaliação. Depois disso, será possível configurar o AWS Control Tower com êxito.

> **Note**
>
> O pacote de conformidade também funciona em situações em que as contas estão localizadas OUs registradas pela AWS Control Tower, mas as cargas de trabalho são executadas em AWS regiões que não têm suporte da AWS Control Tower. É possível usar o pacote de conformidade para gerenciar recursos em contas que existem em regiões onde o AWS Control Tower não está implantado.

Se a conta não atender aos pré-requisitos

Lembre-se de que, como pré-requisito, as contas elegíveis para serem inscritas na governança do AWS Control Tower devem fazer parte da mesma organização geral. Para cumprir esse pré-requisito de inscrição da conta, você pode seguir estas etapas preparatórias a fim de mover uma conta para a mesma organização do AWS Control Tower.

Etapas preparatórias para colocar uma conta na mesma organização do AWS Control Tower

1. Retire a conta da organização existente. Você deverá fornecer uma forma de pagamento separada se usar essa abordagem.
2. Convide a conta para se juntar à organização do 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 e estabelece SCPs e consolida o faturamento.

> **Tip**
>
> Você pode enviar o convite para a nova organização antes que a conta seja retirada da organização antiga. O convite estará aguardando quando a conta for retirada oficialmente de sua organização existente.

Etapas para cumprir os pré-requisitos restantes:

1. Crie os perfis do `AWSControlTowerExecution` necessários.
2. Limpe a VPC padrão. (Essa parte é opcional. O AWS Control Tower não altera a VPC padrão existente.)
3. Exclua ou modifique qualquer gravador AWS Config de configuração ou canal de entrega existente por meio do AWS CLI ou AWS CloudShell. Consulte mais informações em Exemplo de comandos AWS Config CLI para status de recursos e Inscrever contas que tenham recursos do AWS Config existentes

Depois de concluir essas etapas preparatórias, você poderá inscrever a conta no AWS Control Tower. Para obter mais informações, consulte Etapas para inscrever uma conta. Essa etapa coloca a conta na governança completa do AWS Control Tower.

Etapas opcionais para desprovisionar uma conta, para que ela possa ser inscrita 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 apenas o produto provisionado do 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. Depois, 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, depois, encerre-a seguindo as etapas de encerramento da conta em Cancelar a inscrição de uma conta.
5. Se tiver uma OU suspensa com controles definidos, você poderá mover a conta para lá em vez de executar a Etapa 1.

Exemplo de comandos AWS Config CLI para status de recursos

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`

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`

Adicionar manualmente o perfil do IAM necessário a uma Conta da AWS existente e inscrevê-la

Se já configurou a zona de pouso do AWS Control Tower, você pode começar a inscrever as contas da organização em uma UO registrada no AWS Control Tower. Se você não configurou a zona de pouso, siga as etapas descritas no Guia do usuário do AWS Control Tower em Getting Started, Etapa 2. Depois que a zona de pouso estiver pronta, conclua as etapas a seguir para colocar as contas existentes na governança do AWS Control Tower manualmente.

Certifique-se de revisar os Pré-requisitos da inscrição mencionados anteriormente neste capítulo.

Antes de inscrever uma conta no AWS Control Tower, você deve dar permissão ao AWS Control Tower para gerenciar essa conta. Para fazer isso, adicione um perfil que tenha acesso total à conta, conforme mostrado nas etapas a seguir. Essas etapas devem ser realizadas em 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 função do IAM entre contas para fazer login, siga estas etapas:

1. Faça login na conta de gerenciamento da organização.
2. Acesse AWS Organizations.
3. Em Contas, selecione a conta que você deseja inscrever e copie o ID da conta.
4. Abra o menu suspenso da conta na barra de navegação superior e escolha Mudar de perfil.
5. No formulário Mudar de perfil, preencha os seguintes campos:
   - Em Conta, insira o ID da conta que você copiou.
   - Em Perfil, insira o nome do perfil do IAM que permite o acesso entre contas a essa conta. O nome desse perfil foi definido quando a conta foi criada. Se você não especificou um nome de perfil ao criar a conta, insira o nome de perfil padrão, `OrganizationAccountAccessRole`.
6. Selecione Mudar de perfil.

7. Agora você deve estar conectado AWS Management Console à conta de criança.
8. Ao terminar, permaneça na conta secundária durante a próxima parte do procedimento.
9. Anote o ID da conta de gerenciamento, pois será necessário inseri-lo na próxima etapa.

Etapa 2: dê permissão ao AWS Control Tower para gerenciar a conta.

1. Acesse o IAM.
2. Abra Perfis.
3. Selecione Criar perfil.
4. Quando for solicitado que você selecione para qual serviço o perfil 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 *`Management Account ID`* pelo ID real 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. Ignore esta tela por enquanto escolhendo Próximo: revisão
9. Na página Revisão, no campo Nome do perfil, insira `AWSControlTowerExecution`.
10. Insira uma breve descrição na caixa Descrição, como Permite acesso total à conta para inscrição.
11. Selecione Criar perfil.

Etapa 3: inscreva a conta movendo-a para uma UO registrada e verifique a inscrição.

Depois de configurar as permissões necessárias criando o perfil, siga estas etapas para registrar a conta e verificar a inscrição.

1. Faça login novamente como administrador e acesse o AWS Control Tower.
2. Registre a conta.
   - Na página Organização no AWS Control Tower, selecione sua conta e escolha Inscrever no menu suspenso Ações no canto superior direito.
   - Siga as etapas para inscrever uma conta individual, conforme mostrado na página Etapas para inscrever uma conta.
3. Verifique a inscrição.
   - No AWS Control Tower, escolha Organização no painel de navegação à esquerda.
   - Procure a conta que você inscreveu recentemente. Seu estado inicial mostrará o status Inscrevendo.
   - Quando o estado muda para Inscrita, a mudança foi bem-sucedida.

Para continuar esse processo, faça login em cada conta da organização que você deseja inscrever no AWS Control Tower. Repita as etapas de pré-requisito e as etapas de inscrição para cada conta.

Inscrição automática de contas do AWS Organizations

Você pode usar o método de inscrição descrito em uma postagem de blog chamada Inscrever AWS contas existentes no AWS Control Tower para inscrever suas AWS Organizations contas no AWS Control Tower com um processo programático.

O modelo YAML a seguir pode ajudar a criar o perfil necessário em uma conta, para que ela possa ser inscrita 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 do AWS Config existentes

Este tópico fornece uma step-by-step abordagem sobre como inscrever contas que tenham AWS Config recursos existentes. Consulte exemplos de como verificar seus recursos existentes em Exemplo de comandos AWS Config CLI para status de recursos.

> **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 ser contas de auditoria e de arquivamento de logs, 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 zona de pouso do AWS Control Tower
- Sua conta ainda não está inscrita 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 tíquete de suporte para todas as contas que deseja inscrever, conforme descrito em Etapa 1: entre em contato com o suporte ao cliente com um tíquete para adicionar a conta à lista de permissões do AWS Control Tower, a seguir.

Limitações

- A conta só pode ser inscrita 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, a inscrição 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 outra UO 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 cinco etapas principais.

1. Adicione a conta à lista de permissões do AWS Control Tower.
2. Crie um perfil do IAM na conta.
3. Modifique os AWS Config recursos pré-existentes.
4. Crie AWS Config recursos em AWS regiões onde eles não existem.
5. Inscreva a conta no AWS Control Tower.

Antes de prosseguir, considere as expectativas a seguir 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 tíquete para adicionar a conta à lista de permissões do AWS Control Tower

Inclua esta frase na linha de assunto do tíquete:

Inscreva contas que tenham AWS Config recursos existentes no AWS Control Tower

Inclua os seguintes detalhes no corpo do tíquete:

- Número da conta de gerenciamento
- Números de contas de membros que têm AWS Config recursos existentes
- A região de origem selecionada para a configuração do AWS Control Tower

> **Note**
>
> O tempo necessário para adicionar a conta à lista de permissões é de dois dias úteis.

Etapa 2: crie um perfil do IAM na conta-membro.

1. Abra o AWS CloudFormation console da conta do membro.
2. Criar uma pilha usando o modelo a seguir

```
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 CustomerCreatedConfigRecorderRoleForControlTower
4. Crie a pilha.

> **Note**
>
> Qualquer um 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 aviso `AccessDeniedException` quando tiver SCPs esse bloqueio `aws-controltower-ConfigRecorderRole*` de chamar o 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: modifique os recursos existentes em cada região da AWS

Para essa etapa, são necessárias as informações a seguir sobre a configuração do AWS Control Tower.

- `LOGGING_ACCOUNT`: o ID da conta de arquivamento de logs
- `AUDIT_ACCOUNT`: o ID da conta de auditoria
- `IAM_ROLE_ARN`: o ARN do perfil do IAM criado na Etapa 1
- `ORGANIZATION_ID`: é o ID da conta de gerenciamento da organização
- `MEMBER_ACCOUNT_NUMBER`: a conta-membro que está sendo modificada
- `HOME_REGION`: a região de origem da configuração do AWS Control Tower.

Modifique cada recurso existente seguindo as instruções fornecidas nas seções de 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 o item `GLOBAL_RESOURCE_RECORDING` por verdadeiro em sua região de origem. 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 existir outro, modifique as configurações conforme exibido.

- 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`
- S3: KeyPrefix *ORGANIZATION_ID*
- 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 do AWS Control Tower como a região autorizada. Se não existir, crie uma 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 administradas pelo 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 o item GLOBAL_RESOURCE_RECORDING por verdadeiro em sua região de origem. Substitua o item por false para outras regiões onde não 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 e *LOGGING_ACCOUNT_ID* *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 o *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: registre a UO com o AWS Control Tower

No painel do AWS Control Tower, registre a UO.

> **Note**
>
> O fluxo de trabalho Inscrever conta não será bem-sucedido para essa tarefa. Você deve escolher Registrar UO ou Registrar OU novamente.

Provisione e gerencie contas com o Account Factory

Este capítulo inclui uma visão geral e procedimentos para provisionar novas contas-membros em uma zona de pouso do 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 Centro de Identidade do IAM que provisionam contas devem estar no grupo `AWSAccountFactory` ou no grupo de gerenciamento.

> **Note**
>
> Tenha cuidado ao trabalhar com a conta de gerenciamento, como faria ao usar qualquer conta que tenha permissões em toda a organização.

A conta de gerenciamento do AWS Control Tower tem uma relação de confiança com o perfil `AWSControlTowerExecution`, que permite a configuração da conta pela conta de gerenciamento, incluindo algumas configurações de conta automatizadas. Consulte mais informações sobre o perfil `AWSControlTowerExecution` em Roles and accounts.

> **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 obrigatórias 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 chamado de provisionamento avançado de conta ou provisionamento manual de conta. Opcionalmente, você pode provisionar contas programaticamente, com a 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 esquemas personalizados. Consulte mais informações sobre personalização em Personalizar contas com Account Factory Customization (AFC).

Como provisionar contas individualmente no Account Factory, como usuário

1. Faça login no URL do portal do usuário.
2. Em Suas aplicações, escolha Conta da AWS .
3. Na lista de contas, escolha o ID da conta de gerenciamento. Esse 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. Certifique-se de ter selecionado as contas corretas Região da AWS para provisionamento, que devem ser sua região da AWS Control Tower.
6. Procure e escolha Service Catalog para abrir o console do Service Catalog.
7. No painel de navegação, escolha Produtos.
8. Selecione Account Factory do AWS Control Tower e escolha o botão Iniciar produto. Essa ação inicia o assistente para provisionar uma nova conta.
9. Preencha as informações e lembre-se do seguinte:
   - O SSOUsere-mail pode 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 SSOUserE-mail, 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. Quando terminar, escolha Iniciar produto.

11. Revise as configurações da sua conta e escolha Launch (Iniciar). Não crie um plano de recursos, ou sua conta pode não ser 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**
>
> É possível provisionar até cinco contas por vez.

Considerações para gerenciar contas no Account Factory

Você pode atualizar, cancelar a inscrição e encerrar contas criadas e provisionadas por meio do Account Factory. É possível reciclar contas atualizando os parâmetros do usuário nas contas que você deseja reutilizar. Você também pode alterar a unidade organizacional (UO) 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 AWS IAM Identity Center, o AWS Control Tower criará um novo usuário no IAM Identity Center. A conta criada anteriormente não é removida. Consulte informações sobre como remover o endereço de e-mail anterior do usuário do Centro de Identidade do IAM em Desabilitar o acesso dos usuários a Contas da AWS e a aplicações no IAM Identity Center.

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 inscrita é por meio do console do AWS Control Tower. Atualizações de contas individuais são úteis para resolver desvios, como Conta de membro movida. As atualizações da conta também são necessárias como parte de uma atualização completa da zona de pouso.

Se você mover uma conta de uma unidade organizacional (UO) para outra, lembre-se de que os controles aplicados pela nova UO podem ser diferentes dos controles na antiga UO. Os controles na nova UO devem atender aos requisitos da política da conta.

Controle o comportamento quando as contas são movidas entre OUs

Quando você move uma conta entre OUs, os controles para a OU de destino são aplicados ao conta. No entanto, os controles aplicados à conta da antiga UO não são removidos. O comportamento exato dos controles é específico para a implementação do controles que estão ativos na antiga UO e na UO 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 com SCPs: Os controles baseados em SCP da OU anterior são removido. Os controles baseados em SCP para a UO de destino entram em vigor nessa conta.
- Para controles implementados com hooks do AWS CloudFormation : esse comportamento depende do status dos controles na nova UO.
  - Se a UO de destino não tiver controles baseados em hook ativos: os controles antigos permanecem ativos para a conta movida, a menos que você os remova manualmente.
  - Se a UO de destino tiver controles de hook ativos: os controles antigos são removidos e os controles na UO de destino são aplicados à conta.

Atualizar a conta no console

Como atualizar uma conta no console do AWS Control Tower

1. Ao fazer login no AWS Control Tower, acesse 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. Depois, você verá a página Detalhes da conta da conta selecionada.
4. No canto superior direito, escolha Atualizar conta.

Atualizar o produto provisionado

O procedimento a seguir orienta você sobre como atualizar sua conta no Account Factory ou movê-la para uma nova UO, atualizando o produto provisionado da conta no Service Catalog.

Como atualizar uma conta do Account Factory ou alterar sua UO 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 do Centro de Identidade do IAM nos grupos `AWSAccountFactory` ou `AWSServiceCatalogAdmins`).

2. No painel de navegação, escolha Provisionamento e Produtos provisionados.
3. Para cada conta-membro listada, siga as seguintes etapas para atualizar todas as contas-membros:

   a. Selecione uma conta de membro. É aberta a página Detalhes do produto provisionado dessa conta.

   b. Na página Detalhes do produto provisionado, escolha a guia Eventos.

   c. Anote os seguintes parâmetros:

      - SSOUserE-mail (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 da 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 o endereço de e-mail de uma conta inscrita

Para alterar o endereço de e-mail de uma conta-membro inscrita 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 arquivo de logs 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.

Como alterar o endereço de e-mail de uma conta que o AWS Control Tower cria

1. Recupere a senha do usuário-raiz 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 de usuário-raiz.
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 no 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-membro que você criou com o AWS Organizations, consulte Accessing a member account as the root user no Guia do usuário do AWS Organizations .

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. Consulte

mais informações em Updating the root user email address for a member account with AWS Organizations no Guia do usuário do AWS Organizations .

Alterar o nome de uma conta inscrita

Siga o procedimento nesta seção para alterar o nome de uma conta inscrita no 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.

Como alterar o nome de uma conta criada pelo 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 outra Conta da AWS.
5. O AWS Control Tower se atualiza automaticamente para refletir a alteração do nome. Essa atualização não será refletida no produto provisionado no AWS Service Catalog.

Definir o Account Factory com as configurações da Amazon Virtual Private Cloud

O Account Factory permite que você crie linhas de base pré-aprovadas e opções de configuração 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

É possível visualizar as opções de configuração da Amazon VPC disponíveis para os usuários finais quando eles provisionam novas contas.

Como definir as configurações da Amazon VPC no 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 acessar a página de configuração de rede do Account Factory. Lá é possível ver as configurações de rede padrão exibidas. Para editar, selecione Editar e visualize a versão editável das definições de configuração de rede do Account Factory.
3. Você pode modificar cada campo das configurações padrão conforme necessário. Escolha as opções de configuração da VPC que deseja estabelecer para todas as novas contas do Account Factory que os usuários finais possam criar e insira as configurações nos campos.

- Escolha desabilitado ou habilitado para criar uma sub-rede pública na Amazon VPC. Por padrão, a sub-rede com acesso à Internet não é permitida.

> **Note**
>
> Se você definir a configuração da VPC da fábrica de contas para que as sub-redes públicas sejam habilitadas ao provisionar uma nova conta, a fábrica de contas configurará a Amazon VPC para criar um gateway NAT. Você será cobrado pelo uso da Amazon VPC. Consulte Definição de preço da VPC para obter mais informações.

- Escolha o número máximo de sub-redes privadas na Amazon VPC na lista. Por padrão, 1 está selecionado. O número máximo de sub-redes privadas permitidas é 2 por zona de disponibilidade.
- Insira o intervalo de endereços IP para criar sua conta VPCs. O valor deve estar no formato de bloco de roteamento entre domínios sem classe (CIDR) (por exemplo, o padrão é `172.31.0.0/16`). Esse bloco CIDR fornece o intervalo geral de endereços IP de sub-rede para a VPC que o Account Factory cria para sua conta. Dentro da VPC, as sub-redes são atribuídas automaticamente do intervalo especificado, e são iguais em tamanho. Por padrão, as sub-redes dentro da 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 ou todas as regiões para a criação de 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 as quais configurar sub-redes em cada VPC. O número padrão e recomendado é 3.
- Escolha Salvar.

Você pode definir essas opções de configuração para criar contas que não incluam uma VPC. 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 do AWS Control Tower.

Quando você cancela a inscrição de uma conta do AWS Control Tower, todos os recursos provisionados pelo AWS Control Tower são removidos, incluindo os esquemas. A conta é movida de qualquer UO do AWS Control Tower para a área Raiz. A conta não faz mais parte de uma OU registrada e não está mais sujeita ao AWS Control Tower SCPs. Você pode encerrar a conta pelo AWS Organizations.

O cancelamento da inscrição de uma conta também pode ser feito no console do Service Catalog por um usuário do Centro de Identidade do IAM no grupo `AWSAccountFactory`, encerrando o produto provisionado. 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.

Como cancelar a inscrição de uma conta inscrita

1. Abra o console do Service Catalog no navegador da web em https://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 o 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 Account Factory do Service Catalog, a conta não é encerrada. Essa ação remove a conta da UO e da zona de pouso.

6. Quado a inscrição da conta é cancelada, seu status muda para Não inscrita.
7. Se não precisa mais da conta, encerre-a. Para obter mais informações sobre o fechamento de AWS contas, consulte Fechar uma conta no Guia AWS Billing do usuário

Quando você cancela a inscrição de uma conta personalizada, o AWS Control Tower remove os recursos que o esquema implantou, bem como quaisquer outros recursos que o AWS Control Tower criou na conta. Depois de cancelar a inscrição da conta, você pode encerrar a conta por meio do AWS Organizations.

> **Note**
>
> Uma conta não inscrita não é encerrada nem excluída. Quando a inscrição da conta é cancelada, o usuário do Centro de Identidade do IAM que você selecionou ao criar a conta no Account Factory ainda tem acesso administrativo à conta. Se não quiser que esse usuário tenha acesso administrativo, você deverá alterar essa configuração no Centro de Identidade do IAM atualizando a conta no Account Factory e alterando o endereço de e-mail do usuário do Centro de Identidade do IAM para a 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 raiz à conta e, por fim, encerrar a Conta da AWS. Você também pode encerrar uma conta com uma API do AWS Organizations. 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 encerramento de uma conta no AWS Control Tower.

Você pode ver uma lista de AWS YouTube vídeos que explicam tarefas comuns no AWS Control Tower.

Encerrar uma conta criada no Account Factory

As contas criadas no Account Factory são Contas da AWS. Consulte informações sobre o encerramento de Contas da AWS em Closing an account no Guia de referência de gerenciamento de contas da AWS .

> **Note**
>
> Fechar uma não Conta da AWS é o mesmo que cancelar a inscrição de uma conta no AWS Control Tower — essas são ações separadas. Você deve cancelar a inscrição da conta antes de encerrá-la.

Encerrar uma conta-membro do AWS Control Tower por meio do 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 fazer login em cada conta membro individualmente com credenciais raiz, por meio de AWS Organizations. No entanto, você não pode encerrar a conta de gerenciamento dessa forma.

Quando você liga para o AWS Organizations CloseAccount Com a API ou 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 no AWS Control Tower e no AWS Organizations. Se você tentar trabalhar com a conta durante esses 90 dias, o AWS Control Tower emitirá 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.

Aconselhamos, como prática recomendada, a cancelar a inscrição de uma conta-membro antes de encerrar essa conta. Se você encerrar uma conta membro sem antes cancelar o gerenciamento dela, o AWS Control Tower mostrará o status da conta como Suspensa, mas também como Inscrita. Como resultado, se você tentar Registrar novamente a UO da conta durante esse período de 90 dias, o AWS Control Tower gerará 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 UO e mova a conta para essa UO antes de tentar registrar novamente. Recomendamos chamar essa UO de 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-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* 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

AWS serviço	Tipo de recurso	Nome do recurso
		/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Perfis	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole 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 EventBridge	Regra	AWSControlTowerManagedRule
Amazon EventBridge	Regra	aws-controltower-ConfigComplianceChangeEventRule

Personalizar 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 do Account Factory, 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.

Provisione novas contas com plantas

Suas contas personalizadas são provisionadas na AWS Control Tower Account Factory, por meio de AWS CloudFormation modelos ou com o Terraform. Você definirá um modelo que serve como esquema de conta personalizado. O esquema descreve os recursos e as configurações específicos que são necessários quando uma conta é provisionada. Planos predefinidos, criados e gerenciados por AWS parceiros, também estão disponíveis. Consulte mais informações sobre esquemas gerenciados por parceiros em AWS Service Catalog Getting Started Library.

Aplicar esquemas às contas existentes

Você também pode aplicar esquemas personalizados às contas existentes seguindo as etapas de Atualizar conta no console do AWS Control Tower. Para obter detalhes, consulte Atualizar a conta no console.

Definição: Sua conta central

Os planos da sua conta são armazenados em uma Conta da AWS, que, para nossos propósitos, é chamada de conta hub. Os esquemas são armazenados na forma de um produto do Service Catalog. Chamamos esse produto de esquema, para diferenciá-lo de qualquer outro produto do Service Catalog. Consulte mais sobre como criar produtos do Service Catalog em Creating products no Guia do administrador do AWS Service Catalog .

> **Note**
>
> O AWS Control Tower contém controles proativos, que monitoram recursos do AWS CloudFormation no AWS Control Tower. Opcionalmente, você pode ativar esses controles na zona de pouso. 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 organização. Consulte mais informações sobre controles proativos em Proactive controls.

Consulte mais informações sobre como trabalhar com o AFC em Automate account customization using Account Factory Customization in AWS Control Tower.

> **Pré-requisitos**
>
> Antes de começar a criar contas personalizadas com o Account Factory do AWS Control Tower, você deve ter um ambiente de zona de pouso do AWS Control Tower implantado e uma unidade organizacional (UO) registrada no AWS Control Tower, onde suas contas recém-criadas serão colocadas.

Preparação para personalização

- Designe uma conta hub: você pode criar uma nova conta para servir como conta hub ou usar uma existente Conta da AWS. É altamente recomendável não usar a conta de gerenciamento do AWS Control Tower como conta central do esquema.
- Adicione a função necessária: se você planeja se inscrever Contas da AWS na AWS Control Tower e personalizá-la, primeiro você deve adicionar a `AWSControlTowerExecution` função a essas contas, como faria com qualquer outra conta que você esteja inscrevendo na AWS Control Tower.
- Configurar planos de parceiros (opcional): Se você planeja usar planos de parceiros que tenham requisitos de assinatura do Marketplace, você deve configurá-los na sua conta de gerenciamento do AWS Control Tower antes de implantar os planos de parceiros como planos de personalização de fábrica de contas.

Tópicos

- Em caso de erro de esquema
- Personalizando seu documento de política para esquemas do AFC com base em CloudFormation
- Permissões adicionais necessárias para criar um produto do Service Catalog baseado no Terraform

Configuração para personalização

As seções a seguir fornecem etapas para configurar o Account Factory para o processo de personalização. Recomendamos que você configure o administrador delegado para a conta central antes de iniciar essas etapas.

Resumo

- Etapa 1. Crie o perfil exigido. Crie um perfil do IAM que conceda permissão para que o AWS Control Tower tenha acesso à conta (central), onde os produtos do Service Catalog, também chamados de esquemas, são armazenados.
- Etapa 2. Crie o AWS Service Catalog produto. Crie o produto do AWS Service Catalog (também chamado de “produto do esquema”) que você precisará para definir a linha de base da conta personalizada.
- Etapa 3. Revise seu esquema personalizado. Inspecione o AWS Service Catalog produto (blueprint) que você criou.
- Etapa 4. Chame seu esquema para criar uma conta personalizada. Insira as informações do produto do esquema e as informações do perfil nos campos apropriados no Account Factory, no console do AWS Control Tower, ao criar a conta.

Etapa 1. Crie o perfil exigido

Antes de começar a personalizar contas, você deve configurar um perfil que contenha uma relação de confiança entre o AWS Control Tower e sua conta central. Quando assumido, o perfil concede ao AWS Control Tower acesso para administrar a conta central. 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 o perfil `AWSControlTowerBlueprintAccess`, conforme explicado nas seções a seguir. Você pode configurar a função em uma conta inscrita ou não inscrita.

Acesse o console do IAM para configurar o perfil necessário.

Para configurar a AWSControl TowerBlueprintAccess função em uma conta registrada do AWS Control Tower

1. Federar ou fazer login como entidade principal na conta de gerenciamento do AWS Control Tower.
2. Da entidade principal federada na conta de gerenciamento, assuma ou troque os perfis para o perfil `AWSControlTowerExecution` na conta inscrita do AWS Control Tower que você selecionou para servir como a conta central do esquema.
3. Pelo perfil `AWSControlTowerExecution` na conta inscrita do AWS Control Tower, crie o perfil `AWSControlTowerBlueprintAccess` com relações de confiança e permissões adequadas.

Important

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, o perfil `AWSControlTowerExecution` deve ser usado somente pelo AWS Control Tower.

Se a conta central do esquema não estiver inscrita no AWS Control Tower, o perfil `AWSControlTowerExecution` não existirá na conta e não há necessidade de assumi-lo antes de continuar com a configuração do perfil `AWSControlTowerBlueprintAccess`.

Para configurar a AWSControl TowerBlueprintAccess função em uma conta de membro não inscrito

1. Federe ou faça login como entidade principal na conta que você deseja designar como conta central, por meio de seu método preferido.
2. Ao fazer login como entidade principal na conta, crie o perfil `AWSControlTowerBlueprintAccess` com as relações de confiança e as permissões adequadas.

A AWSControlTowerBlueprintAccessfunção deve ser configurada para conceder confiança a dois diretores:

- A entidade principal (usuário) que executa o AWS Control Tower na conta de gerenciamento desse serviço.
- O perfil nomeado `AWSControlTowerAdmin` na conta de gerenciamento do AWS Control Tower.

Aqui está um exemplo de política de confiança, semelhante à que você precisará incluir para o perfil. Essa política demonstra as práticas recomendadas para conceder acesso com privilégio mínimo. Ao criar sua própria política, substitua o termo *`YourManagementAccountId`* pelo ID da conta real da conta de gerenciamento do AWS Control Tower e substitua o termo *`YourControlTowerUserRole`* pelo identificador do perfil do IAM da 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 necessária

O AWS Control Tower exige que a política gerenciada nomeada `AWSServiceCatalogAdminFullAccess` seja anexada ao perfil `AWSControlTowerBlueprintAccess`. 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 o perfil no console do IAM.

Permissões adicionais podem ser necessárias

- Se você armazena seus esquemas no Amazon S3, o AWS Control Tower também exige a política de permissão `AmazonS3ReadOnlyAccess` para o perfil `AWSControlTowerBlueprintAccess`.
- 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 do Terraform.

Etapa 2. Crie o produto do AWS Service Catalog

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 External, consulte Transição para o tipo de produto External.

Resumo das etapas para criar um esquema

- 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 Fazer upload de novo produto.
- No painel Detalhes do produto, insira os detalhes do seu produto de esquema, como nome e descrição.

- Selecione Usar um arquivo de modelo e Escolher arquivo. Selecione ou cole o modelo ou arquivo de configuração que você desenvolveu ou baixou para usar como seu esquema.
- 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 que ela possui.

```
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: nodejs22.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
           export const handler = async (event, context) => {
             const awsAccountId = context.invokedFunctionArn.split(“:”)[4]
             const connectionString= “fake connection for account ” + awsAccountId;
             const response = {
               statusCode: 200,
```

```
              body: connectionString
            };
          return response;
        };

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 esquema personalizado.

Você pode ver seu blueprint no AWS Service Catalog console. Consulte mais informações em Managing products no Guia do administrador do Service Catalog.

Etapa 4. Chame seu esquema 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 esquema que gostaria de usar para personalizar contas.

> **Pré-requisitos**
>
> Você deve configurar sua conta central de personalização e adicionar pelo menos um esquema (produto do 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 esquemas.
2. Nessa conta, selecione um produto existente do Service Catalog (esquema existente).
3. Selecione a versão adequada do esquema (produto do Service Catalog), se você tiver mais de uma versão.
4. (Opcional) Você pode adicionar ou alterar uma política de provisionamento de esquema nesse momento do processo. A política de provisionamento do esquema é escrita em JSON e anexada a um perfil do IAM, para que ele possa provisionar os recursos especificados no modelo do esquema. 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. O perfil é chamado `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*. A política `AdministratorAccess` 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 esquema 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 esquemas ainda não estiverem prontos.

Consulte mais detalhes em Criar uma conta personalizada com base em um esquema.

Criar uma conta personalizada com base em um esquema

Depois de criar esquemas personalizados, você pode começar a criar contas personalizadas no Account Factory do AWS Control Tower.

Siga as etapas a seguir para implantar um esquema personalizado ao criar uma conta da AWS :

1. Acesse o AWS Control Tower no AWS Management Console.
2. Selecione Account Factory e Criar conta.
3. Insira os detalhes da conta, como nome da conta e endereço de e-mail.
4. Configure os detalhes do Centro de Identidade do IAM com endereço de e-mail e nome de usuário.

5. Selecione uma UO registrada na qual sua conta será adicionada.
6. Expanda a seção Account Factory Customization.
7. Insira o ID da conta central do esquema que contém seus produtos do Service Catalog e escolha Validar. Consulte mais informações sobre a conta central do esquema em Personalizar contas com Account Factory Customization (AFC).
8. Selecione o menu suspenso que contém todos os esquemas da sua lista de produtos do Service Catalog (todos os esquemas personalizados e de parceiros). Escolha um esquema e uma versão correspondente para implantação.
9. Se o seu esquema contiver parâmetros, esses campos serão exibidos para você preencher. Os valores padrão são pré-preenchidos.
10. Por fim, selecione onde você implantará seu esquema, seja na Região de origem ou em Todas as regiões administradas. Recursos globais, como Route 53 ou IAM, talvez precisem ser implantados somente em uma única região. Recursos regionais, como EC2 instâncias da Amazon 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 esquemas 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 conta estiver concluído, os recursos especificados por seu esquema já estarão implantados nela. Consulte os detalhes da conta e do esquema na página Detalhes da conta.

Personalize contas com o AFC à medida que você as inscreve

Como inscrever e personalizar contas no console do AWS Control Tower.

1. Acesse o console do AWS Control Tower e selecione Organização no painel de navegação à esquerda.
2. Você verá uma lista das contas disponíveis. Identifique a conta que você gostaria de inscrever com um esquema personalizado. A coluna Estado dessa conta deve refletir a conta com o status Não inscrita.

3. Selecione o botão de opção à esquerda da conta e escolha o menu suspenso Ações no canto superior direito da tela. Aqui você selecionará a opção Inscrever.
4. Conclua a seção Configuração de acesso com as informações do Centro de Identidade do IAM da conta.
5. Selecione a UO registrada na qual sua conta se tornará membro.
6. Conclua a seção Account Factory Customization 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 do provisionamento da conta na página Organização. Quando a inscrição da conta for concluída, os recursos especificados por seu esquema já estarão implantados nela.

Adicionar um esquema a uma conta do AWS Control Tower

Para adicionar um esquema a uma conta-membro existente do AWS Control Tower, siga o fluxo de trabalho de Atualizar conta no console do AWS Control Tower e escolha um novo esquema para adicionar à conta. Consulte mais informações em Update and move Account Factory accounts with AWS Control Tower or with AWS Service Catalog.

> **Note**
>
> Se você adicionar um novo esquema a uma conta, o esquema existente será substituído.

> **Note**
>
> Um esquema pode ser implantado por conta do AWS Control Tower.

Atualizar um esquema

Os procedimentos a seguir descrevem como atualizar esquemas personalizados e implantá-los.

Como atualizar seus esquemas personalizados

1. Atualize seu AWS CloudFormation modelo ou arquivo tar.gz (blueprint) do Terraform com suas novas configurações.

2. Salve o esquema atualizado como uma nova versão no AWS Service Catalog.

Como implantar seu esquema atualizado

1. Acesse a página Organização no console do AWS Control Tower.
2. Filtre a página Organização por nome e versão do esquema.
3. Siga o processo de Atualizar conta e implante a versão mais recente do esquema em sua conta.

Se a atualização do esquema não for bem-sucedida

O AWS Control Tower permite atualizações do esquema quando o produto provisionado está no estado `AVAILABLE`. Se o produto provisionado estiver em um estado `TAINTED`, 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` Consulte mais informações em Updating provisioned products.
2. Depois, siga o processo de atualização da conta no AWS Control Tower para corrigir o erro de implantação do esquema.

Recomendamos essa etapa manual porque: quando você remove um esquema, isso pode fazer com que os recursos na conta-membro sejam removidos. A remoção de recursos pode afetar suas workloads existentes. Por esse motivo, recomendamos esse método em vez da forma alternativa de atualizar um esquema, que consiste em remover e substituir o esquema original, especialmente se você estiver executando workloads de produção.

Remover um esquema de uma conta

Para remover um esquema de uma conta, siga o fluxo de trabalho Atualizar conta para remover o esquema e retornar a conta às configurações padrão do AWS Control Tower.

Ao inserir o 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 esquema da conta. Você verá uma mensagem de aviso antes do início da ação.

> **Note**
>
> O AWS Control Tower adicionará um esquema a uma conta somente se você selecionar um esquema durante o processo Criar conta ou Atualizar conta.

Esquemas 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 esquemas de parceiros ajudam a personalizar suas contas para casos de uso específicos. Os esquemas de cada parceiro ajudam a criar contas personalizadas, que são pré-configuradas para funcionar com as ofertas de produtos desse parceiro específico.

Consulte uma lista completa dos esquemas de parceiros do AWS Control Tower em Getting Started Library do Service Catalog no console. Pesquise o tipo de fonte Esquemas do AWS Control Tower.

Considerações sobre o 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 o perfil do IAM `AWSControlTowerBlueprintAccess` deve ser criado com o nome, as permissões e a política de confiança adequados.
- O AWS Control Tower oferece duas opções de implantação para esquemas: implantar somente na região de origem ou implantar em todas as regiões administradas pelo 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 permite remover um esquema existente e adicionar um novo em uma única operação de atualização do esquema. Você pode remover um esquema e depois adicionar um novo 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 esquemas, o AWS Control Tower cria um produto

provisionado pelo Account Factory (por meio do Service Catalog) na conta de gerenciamento do AWS Control Tower. Se você estiver especificando a personalização ao criar ou inscrever contas com esquemas, o AWS Control Tower não criará um produto provisionado pelo Account Factory na conta de gerenciamento do AWS Control Tower.

Em caso de erro de esquema

Erro ao aplicar um esquema

Se ocorrer um erro durante o processo de aplicação de um esquema em uma conta: seja uma conta nova ou existente que você esteja inscrevendo no AWS Control Tower: o procedimento de recuperação será o mesmo. A conta existirá, mas não será personalizada nem estará inscrita no AWS Control Tower. Para continuar, siga as etapas para inscrever a conta no AWS Control Tower e adicionar o esquema no momento da inscrição.

Erro ao criar o perfil **`AWSControlTowerBlueprintAccess`** e soluções alternativas

Ao criar o perfil `AWSControlTowerBlueprintAccess` por uma conta do AWS Control Tower, você deve ter feito login como entidade principal usando o perfil `AWSControlTowerExecution`. Se você tiver feito login de qualquer outra forma, a operação `CreateRole` será impedida por uma 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"
        }
```

Estas soluções alternativas estão disponíveis:

- (Mais recomendada) Assuma o perfil `AWSControlTowerExecution` e crie o perfil `AWSControlTowerBlueprintAccess`. Se você escolher essa solução alternativa saia do perfil `AWSControlTowerExecution` 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 essa SCP.
- Edite temporariamente essa SCP para permitir a operação.
- (Altamente não recomendada) Use sua conta de gerenciamento do AWS Control Tower como sua conta central, para que ela não esteja sujeita à 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 esquema personalizado por meio do Account Factory é usar

uma política de permissão total, pois essas políticas são compatíveis com qualquer modelo de esquema.

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 o esquema criar um parâmetro do 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 seção `AllowSsmParameterActions` é específica para o modelo que está sendo habilitado.

Resolver problemas de permissão

Ao habilitar um esquema com uma política restrita, você pode descobrir que não há permissões suficientes para habilitar o esquema. Para resolver esses problemas, revise seu documento de política e atualize as preferências do esquema da conta-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 do Service Catalog baseado no Terraform

Ao criar um produto AWS Service Catalog externo com um arquivo de configuração do Terraform para 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 em seu modelo. Se escolher a política de administração completa padrão, você 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.

Provisionar contas com o Account Factory for Terraform (AFT) do AWS Control Tower

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 backend ocorrerá.

Com o AFT, você cria um arquivo do 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 o framework de provisionamento de contas do AFT e as etapas de personalização da conta.

Pré-requisitos

Ao começar a usar o AFT, você criará o seguinte:

- No AWS Control Tower, crie a OU e, em seguida, a conta de gerenciamento da AFT para seu ambiente AFT. Anote o ID da conta, para que você possa inseri-lo no `main.tf` arquivo posteriormente, ao implantar o AFT com o módulo Terraform. Você pode ver esse ID da conta na página de detalhes do AWS Control Tower Control. Para obter mais informações, consulte a documentação do Terraform.

- Um ou mais `git` repositórios para seu ambiente AFT totalmente implantado. Consulte mais informações em Post-deployment steps for AFT.
- Um ambiente do 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). Veja também a documentação do Terraform.

> **Tip**
>
> Você pode criar a conta de gerenciamento do AFT no console do AWS Control Tower com Create account. Para obter mais informações, consulte Métodos de provisionamento. Além disso, opcionalmente, você pode criar uma pasta de modelos de conta para ajudar a definir suas contas adicionais no aft-account-customizationsrepositório.

Para obter informações sobre Regiões da AWS onde o AFT tem limitações de implantação, consulte Limitações e cotas no AWS Control Tower Limitações de controle e.

A documentação do Terraform contém uma boa visão geral de como configurar o AWS Control Tower Account Factory for Terraform (AFT).

Provisionar uma nova conta com o AFT

Esta seção pressupõe que você já tenha configurado o AFT e sua conta de gerenciamento do AFT e esteja provisionando contas adicionais.

Para provisionar uma nova conta com o AFT, crie um arquivo do Terraform de solicitação de conta. Esse arquivo contém a entrada para os parâmetros no aft-account-requestrepositório. Depois de criar um arquivo do Terraform de solicitação de conta, comece a processar a 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. Consulte mais informações em AFT account provisioning pipeline.

Parâmetros do arquivo do Terraform de solicitação de conta

É necessário incluir os seguintes parâmetros no arquivo do 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 solicitação de Conta da AWS .

- O valor de `module source` é o caminho para o módulo do 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 para `control_tower_parameters` não 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 Tagging AWS Organizations resources no Guia do usuário do AWS Organizations .
- O valor de `change_management_parameters` captura informações adicionais, como por que uma solicitação de conta foi criada e quem a iniciou. 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/-fields/. aft/account-request/custom 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 mais Regras do AWS Config. Os metadados que você coleta com `custom_fields` podem invocar processamento adicional durante o provisionamento e a atualização da conta. Se um campo personalizado for removido da solicitação de conta, ele será removido do SSM Parameter Store da conta fornecida.

- (Opcional) `account_customizations_name` captura a pasta do modelo de conta no aft-account-customizationsrepositório. Consulte mais informações em Account customizations.

Enviar várias solicitações de contas

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 do Terraform de solicitação de conta para cada conta que deseja que o AFT provisione ou distribuir várias solicitações de conta em um único arquivo do 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`.

`ManagedOrganizationalUnit` é o único parâmetro que pode ser atualizado, dentre todos `control_tower_parameters`. No entanto, outros parâmetros que fazem parte do arquivo do Terraform da solicitação de conta podem ser atualizados, como `custom_fields`. Consulte mais informações em Provision a new account with AFT.

> **Note**
>
> A entrada que você fornece para `control_tower_parameters` não 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 o 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.

Account Factory for Terraform (AFT) do AWS Control Tower

Esta seção é para administradores de ambientes do AWS Control Tower que desejam configurar o Account Factory for Terraform (AFT) em seu ambiente atual. Ela descreve como configurar um ambiente do Account Factory for Terraform (AFT) com uma nova conta de gerenciamento dedicada do AFT.

> **Note**
>
> Um módulo Terraform implanta o AFT. Este módulo está disponível no repositório AFT em GitHub, e todo o repositório AFT é considerado o módulo.
> Recomendamos que você consulte os módulos AFT em GitHub vez de clonar o repositório AFT. Dessa forma, você pode controlar e consumir atualizações dos módulos à medida que estiverem disponíveis.

Para obter detalhes sobre os últimos lançamentos 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 ambiente AFT, você deve ter os seguintes recursos disponíveis:

- Uma região de origem para a zona de pouso do AWS Control Tower. Consulte mais informações em How Regiões da AWS work with AWS Control Tower.
- Uma zona de pouso do AWS Control Tower. Consulte mais informações em Plan your AWS Control Tower landing zone.
- Uma conta de gerenciamento do AFT, que você pode provisionar na AWS Control Tower ou provisionar por outros meios e se inscrever na AWS Control Tower.
- Uma versão e distribuição do Terraform. Consulte mais informações em Terraform and AFT versions.
- Um provedor de VCS para rastrear e gerenciar alterações no código e em outros arquivos. Por padrão, o AFT usa AWS CodeCommit. Para obter mais informações, consulte O que é AWS CodeCommit? no Guia do AWS CodeCommit usuário.

  Se você estiver implantando o AFT pela primeira vez e não tiver um CodeCommit repositório existente, deverá escolher um provedor externo de VCS, como ou. GitHub BitBucket Consulte mais informações em Alternatives for version control of source code in AFT.
- Um ambiente de runtime em que você pode executar o módulo do Terraform que instala o AFT.
- Opções de recursos do AFT. Consulte mais informações em Enable feature options.

Configurar e iniciar o Account Factory for Terraform do AWS Control Tower

Essas etapas a seguir presumem que você está familiarizado com o fluxo de trabalho do Terraform. Você também pode aprender mais sobre a implantação do AFT seguindo o laboratório de Introdução ao AFT no site do AWS Workshop Studio.

Etapa 1: inicie a zona de pouso do AWS Control Tower

Conclua as etapas em Getting started with AWS Control Tower. É aqui que você cria a conta de gerenciamento do AWS Control Tower e configura a zona de pouso do AWS Control Tower.

> **Note**
>
> Certifique-se de criar uma função para a conta de gerenciamento do AWS Control Tower que tenha AdministratorAccesscredenciais. Consulte mais informações em:
>
> - Consulte Identidades do IAM (usuários, grupos e perfis) no Guia do usuário do AWS Identity and Access Management

- AdministratorAccessno Guia de referência de políticas AWS gerenciadas

Etapa 2: criar uma nova unidade organizacional para o AFT (altamente recomendado)

Recomendamos que você crie uma OU separada na sua zona de pouso do AWS Control Tower. Essa OU é onde você provisiona a conta de gerenciamento do AFT. Crie a nova OU e a conta de gerenciamento AFT a partir da sua conta de gerenciamento do AWS Control Tower. Consulte mais informações em Create a new OU.

Etapa 3: provisione a conta de gerenciamento do AFT

O AFT exige que você provisione uma AWS conta dedicada às operações de gerenciamento do AFT. Crie a conta de gerenciamento do AFT quando estiver conectado à conta de gerenciamento da AWS Control Tower que está associada à sua zona de pouso da AWS Control Tower. Você pode provisionar a conta de gerenciamento do AFT a partir do console do AWS Control Tower selecionando Criar conta na página da organização ou por outros meios. Para obter mais informações, consulte Provisionar contas com o AWS Service Catalog Account Factory.

> **Note**
>
> Se você criou uma UO separada para o AFT, selecione essa UO ao criar a conta de gerenciamento do AFT.

Pode levar até 30 minutos para provisionar totalmente a conta de gerenciamento do AFT.

Etapa 4: verifique se o ambiente do Terraform está disponível para implantação

Essa 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**
>
> O AFT é compatível com o Terraform versão `1.6.0` ou posterior.

Etapa 5: chame o módulo do Account Factory for Terraform para implantar o AFT

Chame o módulo AFT com a função que você criou para a conta de gerenciamento do AWS Control Tower que tem AdministratorAccesscredenciais. O AWS Control Tower provisiona um módulo do Terraform por meio da conta de gerenciamento do AWS Control Tower, que estabelece toda a infraestrutura necessária para orquestrar solicitações do Account Factory do AWS Control Tower.

Você pode visualizar o módulo AFT no repositório AFT em GitHub. Todo o GitHub repositório é considerado o módulo AFT. Consulte informações sobre as entradas necessárias para executar o módulo do AFT e implantar o AFT no arquivo README. Como alternativa, você pode visualizar o módulo do AFT em Terraform Registry.

O módulo do AFT inclui um parâmetro `aft_enable_vpc` que especifica se o AWS Control Tower provisiona recursos da conta dentro de uma nuvem privada virtual (VPC) na conta de gerenciamento central do AFT. Por padrão, o parâmetro é definido como `true`. Se você definir esse parâmetro como `false`, o AWS Control Tower implanta o AFT sem o uso de uma VPC e recursos de rede privada, como gateways NAT ou endpoints da VPC. Desabilitar `aft_enable_vpc` pode ajudar a reduzir o custo operacional do AFT para alguns padrões de uso.

> **Note**
>
> Reabilitar o parâmetro `aft_enable_vpc` (mudando o valor de `false` para `true`) pode exigir que você execute o comando `terraform apply` duas vezes consecutivas.

Se tiver pipelines em seu ambiente que estão estabelecidos para gerenciar o Terraform, você poderá integrar o módulo do AFT ao fluxo de trabalho existente. Caso contrário, execute o módulo do AFT em qualquer ambiente autenticado com as credenciais necessárias.

O tempo limite faz com que a implantação falhe. Recomendamos o uso de 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. Consulte mais informações em Credenciais de segurança temporárias no IAM no Guia do usuário do AWS Identity and Access Management .

> **Note**
>
> Você pode esperar até 30 minutos para que o AFT termine a implantação por meio do módulo do Terraform.

Etapa 6: gerencie o arquivo de estado do Terraform

Um arquivo de estado do Terraform é gerado quando você implanta o AFT. Esse artefato descreve o estado dos recursos que o Terraform criou. Se você planeja atualizar a versão do AFT, preserve o arquivo de estado do Terraform ou configure um backend do Terraform usando o Amazon S3 e o DynamoDB. O módulo do AFT não gerencia um estado de backend do Terraform.

> **Note**
>
> Você é responsável por proteger o arquivo de estado do Terraform. Algumas variáveis de entrada podem conter valores confidenciais, como uma chave `ssh` privada ou um token do Terraform. Dependendo do 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 infraestrutura do AFT for concluída, siga estas etapas adicionais para concluir o processo de configuração e se preparar para provisionar contas.

Etapa 1: Conclua CodeConnections com o provedor de VCS desejado

Se você escolher um provedor de VCS terceirizado, a AFT estabelecerá CodeConnections e você o confirmará. Consulte Alternativas para controle de versão do código-fonte no AFT saber como configurar o AFT com seu VCS preferido.

A etapa inicial de estabelecer a AWS CodeStar conexão é realizada pela AFT. Você deve confirmar a conexão.

Etapa 2: preencha cada repositório

O AFT exige que você gerencie quatro repositórios:

1. Solicitações de conta: esse repositório lida com a colocação ou atualização de solicitações de conta. Exemplos disponíveis. Consulte mais informações sobre solicitações de conta do AFT em Provisionar uma nova conta com o AFT.
2. Personalizações de provisionamento de contas do AFT: esse repositório gerencia as personalizações que são aplicadas a todas as contas criadas e gerenciadas com o AFT, antes de iniciar o estágio global de personalizações. Exemplos disponíveis. Consulte como criar

personalizações de provisionamento de contas do AFT em Criar sua conta do AFT, provisionando máquina de estado de personalizações.

3. Personalizações globais: esse repositório gerencia personalizações que são aplicadas a todas as contas criadas e gerenciadas com o AFT. Exemplos disponíveis. Para criar personalizações globais do AFT, consulte Aplicar personalizações globais.
4. Personalizações de conta: esse repositório gerencia personalizações que são aplicadas somente a contas específicas criadas e gerenciadas com o AFT. Exemplos disponíveis. Para criar personalizações de contas do AFT, consulte Aplicar personalizações de conta.

O AFT espera 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 do Account Factory for Terraform no repositório github do AFT.

Visão geral do Account Factory for Terraform (AFT) do AWS Control Tower

O Account Factory for Terraform (AFT) configura um pipeline do Terraform para ajudar a provisionar e personalizar contas no AWS Control Tower. O AFT oferece a vantagem do provisionamento de contas baseado no Terraform, ao mesmo tempo que permite controlar contas com o AWS Control Tower.

Com o AFT, você cria um arquivo do Terraform de solicitação de conta para receber a entrada que aciona o fluxo de trabalho do AFT para provisionamento de contas. Depois que o estágio de provisionamento de conta for concluído, o AFT executará automaticamente uma série de etapas antes do início do estágio de personalização de conta. Consulte mais informações em AFT account provisioning pipeline.

O AFT é compatível com Terraform Cloud, Terraform Enterprise e Terraform Community Edition. Com o AFT, é possível iniciar a criação da conta usando um arquivo de entrada e um comando `git push` simples e personalizar contas novas ou existentes. A criação de contas inclui todos os benefícios de governança e personalizações de contas do AWS Control Tower que ajudam você a cumprir os procedimentos de segurança padrão e as diretrizes de conformidade da sua organização.

O AFT permite o rastreamento de solicitações de personalização de conta. Toda vez que você envia uma solicitação de personalização de conta, o AFT gera um token de rastreamento exclusivo que passa por uma máquina de AWS Step Functions estado de personalizações do AFT, 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, é possível ver as cargas úteis que acompanham o token, para que você possa rastrear sua solicitação de personalização de conta em todo o fluxo de trabalho do AFT. 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 é o AWS Step Functions? no Guia do desenvolvedor do AWS Step Functions

O AFT combina 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
- Armazenar metadados da conta e histórico de auditoria
- Aplicar tags no nível da conta
- Adicionar personalizações a todas as contas, a um conjunto de contas ou a contas individuais
- Habilitar opções de recursos

O AFT cria uma conta separada, chamada de conta de gerenciamento do AFT, para implantar os recursos do AFT. Antes de configurar o AFT, você deve ter uma zona de pouso existente do AWS Control Tower. A conta de gerenciamento do AFT não é igual à conta de gerenciamento do AWS Control Tower.

O AFT oferece flexibilidade

- Flexibilidade para sua plataforma: o AFT permite qualquer distribuição do Terraform para implantação inicial e operação contínua: Community Edition, Cloud e Enterprise.
- Flexibilidade para seu sistema de controle de versão: suportes AWS CodeCommit AFT e fontes alternativas de controle de versão por meio de Conexões de código da AWS.

O AFT oferece opções de recursos

É possível habilitar várias opções de recursos, com base nas práticas recomendadas:

- Criação de um nível organizacional CloudTrail para registrar eventos de dados
- Excluindo a VPC AWS padrão para contas
- Inscrevendo contas provisionadas no plano Enterprise Support AWS

> **Note**
>
> O pipeline AFT 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 à personalização automáticos de contas do AWS Control Tower.

Vídeo de demonstração

Este vídeo (7:33) descreve como implantar contas com o Account Factory for Terraform do 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.

Video Walkthrough of Automated Account Provisioning in AWS Control Tower.

Arquitetura do AFT

Ordem de operações

Você executa operações do AFT na conta de gerenciamento do AFT. 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. É possível criar e enviar mais de uma solicitação de conta por vez. O Account Factory processa solicitações em um first-in-first-out pedido. Consulte mais informações em Submit multiple account requests.
2. Cada conta é provisionada. Esse estágio é executado na conta de gerenciamento do AWS Control Tower.
3. As personalizações globais são executadas nos pipelines criados para cada conta fornecida.
4. Se as personalizações forem especificadas nas solicitações iniciais de provisionamento da conta, as personalizações serão executadas somente em contas específicas. Se você tem uma conta que já está provisionada, você deve iniciar outras personalizações manualmente no pipeline da conta.

Account Factory for Terraform do AWS Control Tower: fluxo de trabalho de provisionamento de contas

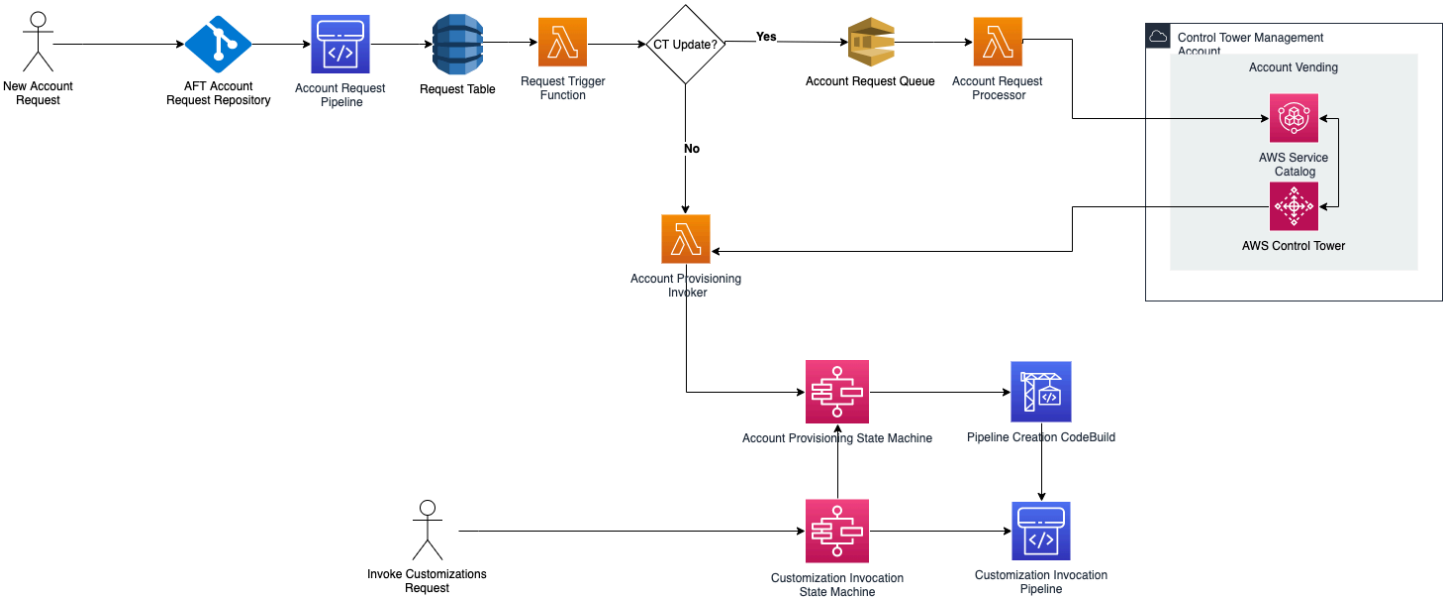

Figura 1: Account Factory for Terraform do AWS Control Tower

Custo

Não há cobrança adicional pelo AFT. Você paga somente pelos recursos implantados pelo AFT, pelos AWS serviços habilitados pelo AFT e pelos recursos implantados no seu ambiente AFT.

A configuração padrão do AFT inclui a alocação de AWS PrivateLink endpoints, para maior proteção e segurança de dados, e um gateway NAT que é necessário para suportar. AWS CodeBuild Consulte detalhes sobre os preços dessa infraestrutura em Preço do AWS PrivateLink e em 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 do AFT.

Versões do AFT e Terraform

O Account Factory for Terraform (AFT) é compatível com o Terraform versão `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 permite três distribuições do Terraform:

- Terraform Community Edition
- Terraform Cloud
- Terraform Enterprise

Essas distribuições serão explicadas nas seções a seguir. Forneça a distribuição do Terraform de sua escolha como um parâmetro de entrada durante o processo de inicialização do AFT. Consulte mais informações sobre a implantação do AFT e os parâmetros de entrada em Account Factory for Terraform (AFT) do AWS Control Tower.

Se você escolher as distribuições Terraform Cloud ou Terraform Enterprise, o token de API especificado para `terraform_token` deverá ser um token de API de usuário ou equipe. Um token de organização não é suportado para todos os itens necessários APIs. Por motivos de segurança, você deve evitar verificar o valor desse token em seu sistema de controle de versão (VCS) atribuindo uma variável do terraform, conforme mostrado no exemplo a seguir.

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

Terraform Community Edition

Quando você seleciona o Terraform Community Edition como distribuição, o AFT gerencia o backend do Terraform para você na conta de gerenciamento do AFT. O AFT baixa a `terraform-cli` da versão especificada do Terraform para ser executada durante a implantação do AFT e as fases do pipeline do AFT. A configuração de estado do Terraform resultante será armazenada em um bucket do 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 excluir funções nesses buckets do Amazon S3 no 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"
```

Terraform Cloud

Quando você seleciona o Terraform Cloud como sua distribuição, o AFT cria áreas 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 pelo AFT
- Personalizações globais para contas provisionadas pelo 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 como confidencial e armazena o valor como uma string segura no armazenamento de parâmetros do SSM na conta de gerenciamento do AFT. Recomendamos que você alterne periodicamente o valor do token do 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 permitidos.
- `terraform_org_name`: esse parâmetro contém o nome da sua organização do Terraform Cloud.

> **Note**
>
> Não há suporte para várias implantações do AFT em uma única organização do Terraform Cloud.

Consulte informações sobre como configurar o Terraform Cloud na documentação do Terraform.

Terraform Enterprise

Quando você seleciona o Terraform Enterprise como sua distribuição, o AFT cria áreas 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 do AFT para contas provisionadas pelo AFT
- Personalizações de conta para contas provisionadas pelo AFT
- Personalizações globais para contas provisionadas pelo 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 do SSM, na conta de gerenciamento do AFT. Recomendamos que você alterne periodicamente o valor do token do 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 do Terraform Enterprise.
- `terraform_api_endpoint`: esse parâmetro contém o URL do seu ambiente do 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.

Verificar a versão do AFT

Você pode verificar sua versão do AFT implantada consultando a chave do 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
}
```

Consulte mais informações sobre as versões do AFT no repositório do AFT.

Atualizar a versão do AFT

Faça login na conta de gerenciamento do AWS Control Tower para iniciar essa atualização do AFT.

Você pode atualizar a versão implantada do AFT retirando-a da ramificação do repositório `main`:

```
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.

Habilitar opções de recursos

O AFT oferece opções de recursos com base nas práticas recomendadas. Você pode optar por esses recursos, por meio de sinalizadores de recursos, durante a implantação do AFT. Consulte mais informações sobre os parâmetros de configuração de entrada do AFT em Provisionar uma nova conta com o AFT.

Esses recursos não são 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 recursos como True em sua configuração da 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. Depois, 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 habilitação 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 a 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 de arquivamento de logs do AWS Control Tower no momento da

habilitação 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 do Enterprise Support, defina o seguinte sinalizador de recursos como True em sua configuração da 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 todos os AWS padrões VPCs na conta de gerenciamento e em todos Regiões da AWS, mesmo que não tenha implantado recursos do AWS Control Tower nelas. Regiões da AWS

O AFT não exclui VPCs automaticamente o 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 de criação 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 recursos como True em sua configuração da entrada de implantação do AFT.

```
aft_feature_delete_default_vpcs_enabled
```

Consulte VPC padrão e sub-redes padrão para saber mais sobre o padrão. VPCs

Considerações sobre recursos do Account Factory for Terraform do AWS Control Tower

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.

Pesquisa de recursos

- Você pode usar tags para pesquisar a lista mais atualizada de recursos do AFT. O par de chave-valor da pesquisa é:

  ```
  Key: managed_by | Value: AFT
  ```

- Para serviços de componentes que não permitem tags, você pode localizar recursos com uma pesquisa por `aft` nos nomes dos recursos.

> **Note**
>
> O AFT não cria nenhum recurso AWS de Backup na conta de gerenciamento.

Tabelas de recursos inicialmente criadas, por conta

Conta de gerenciamento do Account Factory for Terraform do AWS Control Tower

AWS serviço	Tipo de atributo	Nome do recurso
AWS Identity and Access Management	Perfis	AWSAFTAdministrator AWSAFTExecution AWSAFTService

AWS serviço	Tipo de atributo	Nome do recurso
		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-* aws-ct-aft-*
Lambda	Funções	aws-ct-aft-*
Lambda	Camadas	aws-ct-aft-common-layer
DynamoDB	Tabelas	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	Máquinas de estado	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc

AWS serviço	Tipo de atributo	Nome do recurso
Amazon SNS	Tópicos	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	Barramentos de eventos	aws-ct-aft-events-from-ct-management
Amazon EventBridge	Regras de eventos	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
Key Management Service (KMS)	Chaves gerenciadas pelo cliente	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	Parameter Store	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	Filas	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	Grupos de logs	/aws/*/aws-ct-aft-* 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	Perfis	AWSAFTExecution

AWS serviço	Tipo de atributo	Nome do recurso
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	Perfis	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	Parameter Store	/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
AWS Support Center (opcional)	Planos de suporte	Enterprise

Conta de arquivamento de logs do AWS Control Tower

AWS serviço	Tipo de atributo	Nome do recurso
AWS Identity and Access Management	Perfis	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role

AWS serviço	Tipo de atributo	Nome do recurso
Key Management Service (KMS)	Chaves gerenciadas pelo cliente	*-aws-ct-aft-kms-gd-findings
Amazon S3	Buckets	*-aws-ct-aft-logs* 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	Perfis	AWSAFTExecutionRole AWSAFTExecution
AWS Support Center (opcional)	Planos de suporte	Enterprise

Perfis necessários

Em geral, os perfis e as políticas fazem parte do Identity and Access Management (IAM) na AWS. Consulte mais informações no Guia do usuário do AWS IAM.

O AFT cria várias políticas e perfil do IAM nas contas de gerenciamento do AFT e do AWS Control Tower para apoiar as operações do pipeline do AFT. Esses perfis são criados com base no modelo de acesso com privilégio mínimo, que restringe a permissão aos conjuntos mínimos de ações e recursos necessários para cada perfil e política. Essas funções e políticas são atribuídas a um `key:value` par de AWS tags, `managed_by:AFT` para identificação.

Além desses perfis do IAM, o AFT cria três perfis essenciais:

- o perfil `AWSAFTAdmin`
- o perfil `AWSAFTExecution`

- o perfil `AWSAFTService`

Esses perfis são explicados nas seções a seguir.

O AWSAFTAdmin papel, explicado

Quando você implanta o AFT, o perfil `AWSAFTAdmin` é criado na conta de gerenciamento do AFT. Esse perfil permite que o pipeline do AFT assuma o perfil `AWSAFTExecution` 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 em linha (artefato JSON) anexada ao perfil `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 do perfil `AWSAFTAdmin`. O número do espaço reservado `012345678901` é substituído pelo número de ID da conta de gerenciamento do AFT.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

O AWSAFTExecution papel, explicado

Ao implantar o AFT, o perfil `AWSAFTExecution` é criado nas contas de gerenciamento do AFT e do AWS Control Tower. Posteriormente, o pipeline do AFT cria o perfil `AWSAFTExecution` em cada conta provisionada do AFT durante o estágio de provisionamento de conta do AFT.

O AFT utiliza o perfil `AWSControlTowerExecution` inicialmente, para criar o perfil `AWSAFTExecution` em contas especificadas. O perfil `AWSAFTExecution` permite que o pipeline do AFT execute as etapas que são realizadas durante os estágios de provisionamento e personalização do framework do AFT, para contas provisionadas e contas compartilhadas do AFT.

> **Perfis distintos ajudam a limitar o escopo**
>
> Como prática recomendada, mantenha as permissões de personalização separadas das permissões concedidas durante a implantação inicial dos recursos. Lembre-se de que o perfil `AWSAFTService` se destina ao provisionamento de contas e o perfil `AWSAFTExecution` à personalização de contas. Essa separação limita o escopo das permissões concedidas 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) anexada ao perfil `AWSAFTExecution`. O número do espaço reservado `012345678901` é substituído pelo número de ID da conta de gerenciamento do 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

O perfil `AWSAFTService` implanta recursos do AFT em todas as contas registradas e gerenciadas, incluindo as contas compartilhadas e a conta de gerenciamento. Anteriormente, os recursos eram implantados somente pelo perfil `AWSAFTExecution`.

O perfil `AWSAFTService` deve ser usado pela infraestrutura de serviços para implantar recursos durante o estágio de provisionamento, e o perfil `AWSAFTExecution` deve ser usado somente para implantar personalizações. Ao assumir os perfis 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) anexada ao perfil `AWSAFTService`. O número do espaço reservado `012345678901` é substituído pelo número de ID da conta de gerenciamento do 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 implanta o AFT, componentes são adicionados ao seu AWS ambiente a partir de cada um desses AWS serviços.

- AWS Control Tower: o AFT usa o Account Factory do AWS Control Tower na conta de gerenciamento do AWS Control Tower para provisionar contas.
- Amazon DynamoDB: o AFT cria tabelas do Amazon DynamoDB na conta de gerenciamento do AFT, que armazenam solicitações de contas, histórico de auditoria de atualizações da conta, metadados da conta e eventos do ciclo de vida do AWS Control Tower. O AFT também cria gatilhos do Lambda do DynamoDB para iniciar processos posteriores, como iniciar o fluxo de trabalho de provisionamento de contas do AFT.
- Amazon Simple Storage Service — O AFT cria buckets do Amazon Simple Storage Service (S3) na conta de gerenciamento do AFT e na conta de arquivo de log do AWS Control Tower, que armazenam os registros gerados pelos AWS serviços exigidos pelo pipeline do AFT. O AFT também cria um bucket S3 de back-end do Terraform, primário e secundário Regiões da AWS, para armazenar os estados do Terraform gerados durante os fluxos de trabalho do pipeline do AFT.
- Amazon Simple Notification Service: o AFT cria tópicos do Amazon Simple Notification Service (SNS) na conta de gerenciamento do AFT, que armazena notificações de sucesso e falha após processar cada solicitação de conta do AFT. Você pode receber essas mensagens usando o protocolo de sua escolha.
- Amazon Simple Queuing Service: o AFT cria uma fila FIFO do Amazon Simple Queuing Service (Amazon SQS) na conta de gerenciamento do AFT. A fila permite que você envie várias solicitações de conta em paralelo, mas envia uma solicitação por vez ao AWS Control Tower Account Factory, para processamento sequencial.
- AWS CodeBuild — A AFT cria projetos de CodeBuild construção da AWS na conta de gerenciamento da AFT para inicializar, compilar, testar e aplicar planos do Terraform para o código-fonte da AFT em vários estágios de construção.
- AWS CodePipeline — A AFT cria CodePipeline pipelines da AWS na conta de gerenciamento da AFT para se integrar ao seu provedor de CodeStar conexões da AWS selecionado e suportado para o código-fonte da AFT e para acionar trabalhos de construção na AWS CodeBuild.
- AWS Lambda: o AFT cria camadas e funções do AWS Lambda na conta de gerenciamento do AFT para realizar etapas durante a solicitação da conta, o provisionamento da conta do AFT e os processos de personalização da conta.

- O AWS Systems Manager Parameter Store: o AFT configura o AWS Systems Manager Parameter Store na conta de gerenciamento do AFT, para armazenar os parâmetros de configuração necessários para os processos do pipeline do AFT.
- Amazon CloudWatch — A AFT cria grupos de CloudWatch registros da Amazon na conta de gerenciamento da AFT para armazenar registros gerados pelos serviços da AWS empregados pelo pipeline da AFT. O período de retenção CloudWatch dos registros está definido como`Never Expire`.
- Amazon VPC: o AFT cria uma Amazon Virtual Private Cloud (VPC) para isolar serviços e recursos na conta de gerenciamento da AFT em um ambiente de rede separado, para maior segurança.
- AWS KMS: o AFT usa o AWS Key Management Service (KMS) na conta de gerenciamento do AFT e na conta de arquivamento de logs do AWS Control Tower. O AFT cria chaves para criptografar estados do Terraform, dados armazenados em tabelas do DynamoDB e tópicos do SNS. Esses logs e artefatos são gerados quando os recursos e serviços da AWS são implantados pelo AFT. As chaves do KMS criadas pelo AFT têm a rotação anual habilitada por padrão.
- AWS Identity and Access Management (IAM) — O AFT segue o modelo de privilégios mínimos recomendado. Ele cria funções e políticas do AWS Identity and Access Management (IAM) na conta de gerenciamento do AFT, nas contas da AWS Control Tower e nas contas provisionadas do AFT, conforme necessário, para realizar as ações necessárias durante o fluxo de trabalho do pipeline do AFT.
- AWS Step Functions — O AFT cria máquinas de estado do AWS Step Functions na conta de gerenciamento do AFT. Essas máquinas de estado orquestram e automatizam o processo e as etapas da estrutura e das personalizações de provisionamento de contas do AFT.
- Amazon EventBridge — A AFT cria um barramento de EventBridge eventos da Amazon na conta de gerenciamento da AFT e da AWS Control Tower para capturar e armazenar eventos do ciclo de vida da AWS Control Tower a longo prazo na tabela do DynamoDB da conta de gerenciamento da AFT. A AFT cria regras de CloudWatch eventos da Amazon nas contas de gerenciamento da AFT e da AWS Control Tower, que acionam várias etapas necessárias durante a execução do fluxo de trabalho do pipeline da AFT
- AWS CloudTrail (Opcional) — Quando esse recurso é ativado, o AFT cria uma trilha AWS CloudTrail organizacional na conta de gerenciamento do AWS Control Tower, para registrar eventos de dados para buckets do Amazon S3 e funções AWS Lambda. O AFT envia esses logs para um bucket central do S3 na conta de arquivamento de logs do AWS Control Tower.
- AWS Support (opcional) — Quando esse recurso está ativado, o AFT ativa o plano AWS Enterprise Support para contas provisionadas pelo AFT. Por padrão, AWS as contas são criadas com o plano AWS Basic Support ativado.

Pipeline de provisionamento de contas do AFT

Após a conclusão do estágio de provisionamento de contas do pipeline, o framework 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 etapa Personalizações da conta.

Aqui estão as próximas etapas que o pipeline do AFT executa.

1. Valida a entrada da solicitação de 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. O AFT assume esse perfil para realizar o estágio de personalização da conta, porque esse perfil concede acesso ao portfólio do Account Factory.
5. Aplica as tags de conta que você forneceu como parte dos parâmetros de entrada de 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 do 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 repositório `git`. Às vezes, esse estágio é chamado de estágio do framework de provisionamento de contas. Isso faz parte do processo principal de provisionamento, mas você já configurou um framework que fornece integrações personalizadas como parte do fluxo de trabalho de provisionamento de contas, antes que mais personalizações 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 de conta para cada conta provisionada (e direcionada).
10. Envia uma notificação de sucesso ou falha para o tópico do SNS, por meio da qual é possível recuperar as mensagens.

Configurar as personalizações do framework 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 pelo 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 do framework de provisionamento de contas são implementadas em todas as contas provisionadas, antes do próximo estágio global de personalização de conta começar.

> **Note**
>
> O recurso do 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 auxiliares globais no estágio de personalização de conta.

O framework de provisionamento de contas do 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.

- Funções do AWS Lambda na linguagem de sua escolha
- Tarefas do AWS ECS ou AWS Fargate, usando contêineres do Docker
- Atividades do AWS Step Functions usando operadores personalizados, hospedados na AWS ou no ambiente on-premises
- Integrações com o Amazon SNS ou SQS

Se nenhuma máquina de estado do AWS Step Functions for definida, o estágio passa como “sem operação”. Para criar uma máquina de estado de personalizações de provisionamento de contas do AFT, siga as instruções em Criar sua conta do AFT, provisionando máquina de estado de personalizações. Antes de adicionar personalizações, verifique se você tem os pré-requisitos estabelecidos.

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 de contas do AFT. Em vez disso, o pipeline do 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 de contas do AFT, conforme descrito nas seções a seguir.

Pré-requisitos para criar uma máquina de estado

- Um AFT totalmente implantado. Consulte mais informações sobre implantações do AFT em Account Factory for Terraform (AFT) do AWS Control Tower.
- Configure um repositório `git` em seu ambiente para personalizações de provisionamento de contas do AFT. Consulte Etapas de pós-implantação para obter mais informações.

Criar sua conta do AFT, provisionando máquina de estado de personalizações

Etapa 1: modifique a definição da máquina de estado

Modifique o exemplo `customizations.asl.json` de definição da máquina de estado. O exemplo está disponível no repositório `git` que você configurou para armazenar personalizações de provisionamento de contas do 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: inclua a configuração correspondente do Terraform

Inclua arquivos do Terraform com a extensão `.tf` no mesmo repositório `git` com a definição da máquina de estado para sua integração personalizada. Por exemplo, se você optar por chamar uma função do Lambda na definição da tarefa da máquina de estado, inclua o arquivo `lambda.tf` no mesmo diretório. Certifique-se de incluir as permissões e os perfis do IAM necessários para as 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.

Como reiniciar o framework e as personalizações de provisionamento de contas do AFT

O AFT executa a estrutura de provisionamento de contas e as etapas de personalização para cada conta fornecida pelo pipeline do AFT. Para reiniciar as personalizações de provisionamento de conta, você pode usar um destes dois métodos:

1. Faça qualquer alteração em uma conta existente no repositório de solicitações de conta.
2. Provisione uma nova conta com o AFT.

Personalizações da conta

O AFT pode implantar configurações padrão ou personalizadas em contas provisionadas. Na conta de gerenciamento do AFT, o 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 conta.

Visão geral

Depois que suas personalizações forem especificadas nos repositórios `git` escolhidos, seja aquele em que você armazena suas personalizações globais ou onde você armazena as personalizações da conta, o estágio de personalização da conta é concluído automaticamente pelo pipeline do AFT. Para personalizar contas retroativamente, consulte Invocar novamente personalizações.

Personalizações globais (opcional)

Você pode optar por aplicar determinadas personalizações a todas as contas provisionadas pelo AFT. Por exemplo, se você precisar criar um perfil do IAM específico ou implantar um controle personalizado em cada conta, o estágio de personalizações globais no pipeline do AFT permite fazer isso automaticamente.

Personalizações de conta (opcional)

Para personalizar uma conta individual ou um conjunto de contas de forma diferente de outras contas provisionadas pelo AFT, você pode utilizar 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 da internet.

Pré-requisitos de personalização

Antes de começar a personalizar contas, verifique se esses pré-requisitos estão em vigor.

- Um AFT totalmente implantado. Consulte informações sobre como implantar em Configurar e iniciar o Account Factory for Terraform do AWS Control Tower.
- Repositórios `git` pré-preenchidos para personalizações globais e personalizações de contas em seu ambiente. Consulte mais informações em Etapa 3: preencher cada repositório em Etapas de pós-implantação.

Aplicar personalizações globais

Para aplicar personalizações globais, você deve enviar uma estrutura de pastas específica para o repositório escolhido.

- Se as suas configurações personalizadas estiverem na forma de programas ou scripts em Python, coloque-as na pasta api_helpers/python em seu repositório.
- Se as suas configurações personalizadas estiverem na forma de scripts Bash, coloque-as na pasta api_helpers em seu repositório.
- Se as suas configurações personalizadas estiverem no formato do Terraform, coloque-as na pasta terraform em seu repositório.
- Consulte mais detalhes sobre a criação de configurações personalizadas no arquivo README de personalizações globais.

> **Note**
>
> As personalizações globais são aplicadas automaticamente, após o estágio do framework de provisionamento da conta do AFT no pipeline do AFT.

Aplicar personalizações de conta

Você pode aplicar personalizações de conta enviando uma estrutura de pastas específica para o repositório escolhido. As personalizações de 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 que você precisar, use as etapas a seguir.

Como aplicar personalizações de conta

1. Etapa 1: criar uma pasta para uma personalização de conta

   No repositório escolhido, copie a pasta `ACCOUNT_TEMPLATE` 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. Adicionar as configurações à pasta específica de personalizações de conta

   Você pode adicionar configurações à pasta de personalizações de conta com base no formato das configurações.

   - Se suas configurações personalizadas estiverem na forma de programas ou scripts em Python, coloque-as na pasta /api_helpers/python que está ***[account_customizations_name]*** 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.

   Consulte mais informações sobre como criar configurações personalizadas no arquivo README das personalizações de conta.

3. Consultar o parâmetro **`account_customizations_name`** específico no arquivo de solicitação de conta

   O arquivo de solicitação de conta do AFT inclui o parâmetro de entrada `account_customizations_name`. Insira o nome da personalização de 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 entrada `account_customizations_name` em suas solicitações de conta. Consulte mais informações em Submit multiple account requests.

Invocar novamente personalizações

O AFT fornece uma maneira de invocar novamente 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: envie alterações para repositórios **`git`** globais ou de personalizações de contas

Você pode atualizar suas personalizações globais e de conta conforme necessário e enviar as alterações de volta aos repositórios `git`. Neste momento, nada acontece. O pipeline de personalizações deve ser invocado por uma fonte de eventos, conforme explicado nas próximas duas etapas.

Etapa 2: inicie uma execução de função do AWS Step Functions para invocar novamente personalizações

O AFT fornece uma função do AWS Step Functions chamada `aft-invoke-customizations` na conta de gerenciamento do AFT. O objetivo dessa função é invocar novamente o pipeline de personalização para contas provisionadas pelo AFT.

Aqui está um exemplo de um esquema de evento (formato JSON) que você pode criar para passar a entrada para a função `aft-invoke-customizations` do AWS Step Functions.

```
{
  "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 nova invocação. Você pode filtrar por unidade organizacional (UO), tags de conta e ID de conta. Se você não aplicar nenhum filtro e incluir a instrução `"type":"all"`, a personalização de todas as contas provisionadas pelo AFT será invocada novamente.

> **Note**
>
> Se sua versão do AWS Control Tower Account Factory for Terraform (AFT) for 1.6.5 ou posterior, você pode segmentar (aninhado OUs 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, cinco personalizações por vez.

O 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 da Step Function contém uma conta IDs que corresponde à fonte do evento de entrada da 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 de conta do AFT

Fluxos de trabalho de personalização de contas baseados em registros de emissão contendo a conta de destino e a solicitação de AWS Lambda personalização. IDs O AFT permite que você rastreie e solucione 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 pela 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 à esquerda, escolha Logs e, depois, Log Insights.
3. Escolha Consultas.
4. Em Exemplos de consultas, escolha Account Factory for Terraform e selecione uma das seguintes consultas:
   - Logs de personalização por ID da conta

> **Note**
>
> Certifique-se de *"YOUR-ACCOUNT-ID"* substituir 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/
```

- Logs de personalização por ID de solicitação de personalização

> **Note**
>
> Certifique-se de *"YOUR-CUSTOMIZATION-REQUEST-ID"* substituir 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. Consulte mais informações sobre a estrutura de provisionamento de contas do AFT em AFT account provisioning pipeline.

```
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, escolha um intervalo de tempo e selecione Executar consulta.

Alternativas para controle de versão do código-fonte no AFT

O AFT usa AWS CodeCommit 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 o AFT pela primeira vez e não tiver um CodeCommit repositório existente, deverá especificar um provedor externo de VCS, como parte dos pré-requisitos de implantação do AFT. Consulte mais informações em Alternatives for version control of source code in AFT.

O AFT permite as seguintes alternativas de controle de código-fonte:

- GitHub
- GitHub Servidor corporativo
- BitBucket
- GitLab
- GitLab Autogerenciado

> **Note**
>
> Se você especificar AWS CodeCommit como seu VCS, nenhuma etapa adicional será necessária. O AFT cria os repositórios `git` 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.

Configurar um sistema alternativo de controle de versão de código-fonte (VCS personalizado) com o AFT

Para configurar um sistema alternativo de controle de versão de código-fonte para sua implantação do AFT, siga estas etapas.

Etapa 1: crie repositórios **`git`** em um sistema de controle de versão (VCS) de terceiros compatível.

Se você não estiver usando AWS CodeCommit, deverá criar `git` repositórios em seu ambiente de provedor de VCS terceirizado suportado pelo AFT para os seguintes itens.

- Solicitações de conta do AFT. Amostra de código disponível. Consulte mais informações sobre solicitações de conta do AFT em Provisionar uma nova conta com o AFT.
- Personalizações de provisionamento de contas do AFT. Amostra de código disponível. Consulte mais informações sobre personalizações de provisionamento de contas do AFT em Criar sua conta do AFT, provisionando máquina de estado de personalizações.
- Personalizações globais do AFT. Amostra de código disponível. Consulte mais informações sobre personalizações globais do AFT em Personalizações da conta.
- Personalizações da conta do AFT. Amostra de código disponível. Consulte mais informações sobre as etapas de personalização em Personalizações da conta.

Etapa 2: especifique os parâmetros de configuração do VCS necessários para a implantação do AFT

Os seguintes parâmetros de entrada são necessários para configurar seu provedor de VCS como parte da implantação do AFT.

- vcs_provider: Se você não estiver usando AWS CodeCommit, especifique o provedor VCS como`"bitbucket"`,,, ou `"github"` `"githubenterprise"``"gitlab"`, com base no seu caso de uso.
- github_enterprise_url: somente para clientes GitHub corporativos, especifique a URL. GitHub
- account_request_repo_name: para AWS CodeCommit usuários, esse valor é definido como. `aft-account-request` Em um ambiente de provedor de VCS de terceiros compatível com o AFT, atualize esse valor de entrada com o nome real do repositório. Para BitBucket Github, GitHub Enterprise e GitLab Self-managed GitLab, 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 de provedor de VCS de terceiros compatível com o AFT, atualize esse valor de entrada com o nome do repositório. Para BitBucket Github, GitHub Enterprise e GitLab Self-managed GitLab, o nome do repositório deve ter o formato. `[Org]/[Repo]`
- account_provisioning_customizations_repo_name: para usuários do AWS CodeCommit , esse valor é definido como `aft-account-provisioning-customizations`. Em um ambiente de provedor de VCS de terceiros compatível com o AFT, atualize esse valor de entrada com o nome do repositório. Para BitBucket Github, GitHub Enterprise e GitLab Self-managed GitLab, 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 de provedor de VCS de terceiros compatível com o AFT, atualize esse valor de entrada com o nome do repositório. Para BitBucket Github, GitHub Enterprise e GitLab Self-managed GitLab, 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, o AFT é originado da ramificação `main` de cada repositório `git`. Você pode substituir o valor do nome da ramificação por um parâmetro de entrada adicional. Consulte mais informações sobre os parâmetros de entrada no arquivo README no módulo do Terraform do AFT.

> **Para AWS CodeCommit clientes existentes**
>
> Se você criar um CodeCommit repositório com um novo nome para AFT, poderá atualizar o nome do repositório atualizando os valores desses parâmetros de entrada.

Etapa 3: Concluir a AWS CodeStar conexão para provedores de VCS terceirizados

Quando sua implantação é executada, o AFT cria os AWS CodeCommit repositórios necessários ou cria uma AWS CodeStar conexão para o provedor de VCS terceirizado escolhido. No último caso, você deve entrar manualmente no console da conta de gerenciamento do AFT para concluir a AWS CodeStar conexão pendente. Consulte a AWS CodeStar documentação para obter mais instruções sobre como concluir a AWS CodeStar conexão.

Mova o AFT AWS CodeCommit de outro provedor de VCS

Esta seção fornece uma visão geral de como você pode mover o AWS Control Tower Account Factory for Terraform (AFT) do AWS CodeCommit seu sistema de controle de versão (VCS) para outro provedor de VCS.

Etapa 1. Configure novos repositórios no VCS de sua escolha.

Etapa 2. Adicione esses repositórios como novos controles remotos. `git`

Etapa 3. Execute `git push` no novo provedor de VCS.

> **Note**
>
> A estrutura do repositório que você cria deve ser a mesma que em AWS CodeCommit. Alterar a estrutura impede a capacidade do AFT de executar o código desejado.
>
> Estrutura do repositório:
>
> - aft-account-request
> - aft-account-customizations
> - aft-global-customizations
> - aft-account-provisioning-customizations

Etapa 4. Na sua conta de gerenciamento do AWS Control Tower, atualize o módulo Terraform (bootstrap) para apontar para seu provedor de VCS, conforme mostrado no exemplo a seguir:

Exemplo: GitLab com o Terraform OSS

— Execute `terraform plan` para visualizar as alterações, então`terraform apply`.

Etapa 5. Conclua as etapas para concluir a configuração do CodeConnection (anteriormente conhecido como CodeStar):

1. Faça login na sua conta de gerenciamento da AFT
2. Localize e preencha o pendente AWS CodeConnections para o novo provedor VCS, conforme descrito em Atualizar uma conexão pendente [] `https://us-east-1.console.aws.amazon.com/codesuite/settings/connections`
3. Referência: Etapas de pós-implantação

> **Note**
>
> Os pipelines da conta retêm a fonte anterior até que `aft-invoke-customizations` Step Functions seja invocado. Essa invocação pode ser feita como parte da atualização ou como parte das próximas invocações de personalizações.

Para obter mais informações, consulte este blog: Como migrar seu AWS CodeCommit repositório para outro provedor Git.

Proteção de dados

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no AFT. Para fins de proteção de dados, aconselhamos as práticas recomendadas a seguir.

- Siga as diretrizes de proteção de dados fornecidas pelo AWS Control Tower. Para obter detalhes, consulte Proteção de dados no AWS Control Tower.
- Preserve a configuração de estado do Terraform gerada no momento da implantação do AFT. Para obter detalhes, consulte Account Factory for Terraform (AFT) do AWS Control Tower.
- Alterne as credenciais confidenciais periodicamente, conforme indicado pela política de segurança da sua organização. Exemplos de segredos são tokens do Terraform, tokens `git` 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 do KMS criadas pelo AFT têm a rotação anual habilitada 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 do AFT é irreversível e pode resultar em perda de estado.

Você pode remover uma conta do AFT quando quiser fechar a conta de uma aplicação retirada, 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 uma 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 AWS consulte o seguinte:
>
> - Unmanage an account no Guia do usuário do AWS Control Tower.
> - Encerrar uma Conta da AWS no Guia do usuário do AWS Billing .

Como remover uma conta dos pipelines do AFT

O procedimento a seguir descreve como remover uma conta do AFT.

1. Remover conta do repositório **`git`** que armazena solicitações de conta

   No repositório `git` 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. Excluir a área de trabalho do Terraform (somente para clientes do Terraform Cloud e do Terraform Enterprise)

   Exclua as personalizações globais e as áreas de trabalho de personalizações de conta da conta que deseja remover do AFT.
3. Excluir o estado do Terraform do backend 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, substitua *012345678901* pelo número do ID da conta de gerenciamento do AFT.

Exemplo: Terraform OSS

Ao escolher o Terraform OSS, você encontra três pastas para cada conta nos buckets `aft-backend-012345678901-primary-region` e `aft-backend-012345678901-secondary-region` do Amazon 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 Terraform Enterprise, você encontra uma pasta para cada conta nos buckets `aft-backend-012345678901-primary-region` e `aft-backend-012345678901-secondary-region` do Amazon 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. AWS Usamos 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 único universal (UUID): identificador exclusivo gerado aleatoriamente para cada implantação do AFT
- Carimbo de data/hora: carimbo de data/hora da coleta de dados
- Dados: configuração do AFT e ações realizadas pelo cliente

AWS possui os dados coletados. A coleta de dados está sujeita à Política de Privacidade da AWS.

> **Note**
>
> As versões do AFT anteriores à 1.6.0 não relatam métricas de uso para a AWS.

Como desabilitar o relatório de métricas:

- Defina o valor de entrada de `aft_metrics_reporting` como `false` no 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 defini-lo explicitamente.

Se você copiar o exemplo, lembre-se de substituir seus valores reais de ID e região pelos itens fornecidos em strings com `x`.

```
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 ajudar 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 obter mais informações, consulte:

- O que é o AWS CodeBuild? no CodeBuild Guia do usuário
- O que AWS Organizationsé no Guia do Usuário do Organizations.
- O que AWS Systems Manageré no Guia do usuário do Systems Manager.

- Versão desatualizada do Account Factory

  Se encontrar um problema e achar que é um erro, verifique se você tem versão mais recente do Account Factory. Consulte mais informações em Updating the Account Factory version.

- Foram feitas alterações locais no código-fonte do Account Factory

  O 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 permitirá sua implantação do Account Factory com base no melhor esforço.

- Permissões insuficientes do perfil do Account Factory

  O Account Factory cria políticas e perfis do IAM para gerenciar implantações e personalizações de contas fornecidas. Se você alterar esses perfis ou políticas, o pipeline do Account Factory poderá não conseguir realizar determinadas ações. Consulte mais informações em Required roles.

- Repositórios de contas não preenchidos corretamente

  Certifique-se de seguir as etapas de pós-implantação antes de provisionar contas.

- Não é detectado o desvio após alterar a UO manualmente

  > **Note**
  >
  > O AWS Control Tower detecta o desvio automaticamente. Consulte informações sobre como resolver desvios em Detect and resolve drift in AWS Control Tower.

  O desvio não é detectado quando a unidade organizacional (UO) 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 altera a UO manualmente, o desvio não é 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 do Service Catalog durante o provisionamento ou como `ConditionalCheckFailedException`.

  Você pode encontrar mais informações sobre o problema seguindo um destes procedimentos:

  - Revise seus grupos de registros do Terraform ou do CloudWatch Logs.
  - Analise as falhas que são emitidas para o tópico `aft-failure-notifications` do Amazon SNS.
- Solicitação de conta criada incorretamente

  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. Consulte mais informações em Update an existing account.
- Conta que os destinos da solicitação de personalização existem na tabela **`aft-request-metadata`** do DynamoDB, mas não no repositório de solicitações de conta

  Formate sua solicitação de invocação de personalização para excluir a conta incorreta seguindo um destes procedimentos:

  - Na tabela `aft-request-metadata` do DynamoDB, exclua a entrada que faz referência à conta que não está mais no seu repositório de solicitações de conta.
  - Não use “tudo” como destino.
  - Não use como destino a OU à qual a conta pertence.
  - Não use como destino a conta diretamente.
- Usou o token incorreto para o Terraform Cloud

  Verifique se configurou o token correto. O Terraform Cloud é compatível apenas com tokens baseados em equipe, não com 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 no valor de uma tag de 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 posterior 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

Consulte mais informações sobre como verificar e atualizar sua versão do AFT em:

- Check the AFT version
- Update the AFT version

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 sua solicitação de personalização. IDs Consulte mais informações em Troubleshooting with AFT account customization request tracing.

Detectar e resolver desvios no AWS Control Tower

Identificar e resolver desvios é uma tarefa de operações regulares para administradores de contas de gerenciamento do AWS Control Tower. Resolver desvios ajuda a garantir a 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 organização usam a zona de pouso, podem ocorrer alterações no status de conformidade. 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.

Detectar desvios

O AWS Control Tower detecta o desvio automaticamente. Para detectar desvios, o perfil `AWSControlTowerAdmin` exige acesso persistente à conta de gerenciamento para que o AWS Control Tower possa fazer chamadas de API somente para leitura ao AWS Organizations. Essas chamadas de API aparecem como eventos do AWS CloudTrail .

O desvio aparece nas notificações do Amazon Simple Notification Service (Amazon SNS) que são agregadas na conta de auditoria. As notificações em cada conta-membro enviam alertas para um tópico local do Amazon SNS e para uma função do Lambda.

Para controles que fazem parte do padrão AWS Security Hub gerenciado por serviços: AWS Control Tower, o desvio é mostrado nas páginas de conta e detalhes da conta no console do AWS Control Tower, bem como por meio de uma notificação do Amazon SNS.

Os administradores de contas-membros podem (e como melhor prática, devem) assinar notificações de oscilação do SNS para contas específicas. Por exemplo, o tópico `aws-controltower-AggregateSecurityNotifications` do SNS fornece notificações de desvios. O console do AWS Control Tower indica aos administradores da conta de gerenciamento quando o desvio ocorreu. Consulte mais informações sobre tópicos do SNS para detecção e notificação de desvios em Drift prevention and notification.

Deduplicação e notificação de desvios

Se o mesmo tipo de desvio ocorrer no mesmo conjunto de recursos várias vezes, o AWS Control Tower enviará uma notificação do SNS somente para a instância inicial do desvio. Se o AWS Control Tower detectar que essa instância de desvio foi corrigida, ele enviará outra notificação somente se o desvio ocorrer novamente para esses recursos idênticos.

Exemplos: o desvio de conta e o desvio de SCP são tratados da seguinte maneira

- Se você modificar a mesma SCP gerenciada várias vezes, receberá uma notificação na primeira vez em que modificá-la.
- Se você modificar uma SCP gerenciada, corrigir o desvio e modificá-la 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 UO para outra, os controles da UO anterior não são removidos. Se você habilitar qualquer novo controle baseado em hook na UO de destino, o antigo o controle baseado em hook 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 alterada OUs.

Tipos de desvio de política

- SCP atualizada
- SCP anexada à UO
- SCP desanexada da UO
- SCP anexada à conta

Consulte mais informações em Types of Governance Drift.

Resolver desvios

Embora a detecção seja automática, as etapas para resolver o desvio devem ser feitas manualmente por meio do console ou, para controles, chamando a ResetEnabledControlAPI.

- Muitos tipos de desvio podem ser resolvidos na página Configurações de zona inicial. Você pode escolher o botão Redefinir na seção Versões para resolver esses tipos de desvio.
- Se sua UO tiver menos de mil contas, você poderá resolver o desvio nas contas provisionadas pelo Account Factory, ou o desvio da SCP, selecionando Registrar UO novamente na página Organização ou na página de Detalhes da UO.
- Talvez você consiga resolver o desvio de contas, por exemplo Conta de membro movida, atualizando uma conta individual. Para obter mais informações, consulte Atualizar a conta no console.
- Para controles, muitos tipos de desvio podem ser resolvidos chamando a ResetEnabledControlAPI.

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

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

Considerações sobre verificações de desvio e SCP

O AWS Control Tower escaneia seus controles SCPs diariamente para verificar se os controles correspondentes foram aplicados corretamente e se não foram desviados. Para recuperá-los SCPs

e executar verificações sobre eles, o AWS Control Tower liga AWS Organizations em seu nome, usando uma função em sua conta de gerenciamento.

Se uma verificação do AWS Control Tower descobrir um desvio, você receberá uma notificação. O AWS Control Tower envia apenas uma notificação por problema de desvio, portanto, se a zona de pouso já estiver em um estado de desvio, você não receberá notificações adicionais a menos que um novo item de desvio 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 limite de TPS, taxa de controle de utilização ou taxa de solicitação de API. Quando a AWS Control Tower audita sua SCPs chamada AWS Organizations, as chamadas de API que a AWS Control Tower faz são contabilizadas em seu limite de TPS, 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 o AWS Control Tower fizerem a mesma chamada AWS Organizations APIs no mesmo momento (dentro de 1 segundo) e os limites de TPS forem atingidos, as chamadas subsequentes serão limitadas. Ou seja, essas chamadas retornam um erro como `Rate exceeded`.

Se uma taxa de solicitação de API for excedida

- Se o AWS Control Tower atingir o limite e for limitado, pausaremos a execução da auditoria e a retomaremos posteriormente.
- Se a workload atingir o limite e for limitada, o resultado pode variar de uma leve latência até um erro fatal na workload, dependendo de como a workload está configurada. Esse caso extremo é algo que você deve conhecer.

Uma verificação diária da SCP consiste em

1. Recuperando seu recém-ativo OUs.
2. Para cada OU registrada, recuperando todas SCPs gerenciadas pelo AWS Control Tower que estão anexadas à OU. SCPs Os gerenciados têm identificadores que começam com`aws-guardrails`.
3. Para cada controle preventivo ativado na OU, verificando se a declaração de política do controle está presente na UO gerenciada SCPs.

Uma OU pode ter um ou mais gerenciados SCPs.

Tipos de desvio a serem resolvidos imediatamente

A maioria dos tipos de oscilações pode ser resolvida pelos administradores. Alguns tipos de desvio devem ser resolvidos imediatamente, incluindo a exclusão de uma unidade organizacional que a zona de pouso do AWS Control Tower requer. Aqui estão alguns exemplos de grandes desvios que você talvez queira evitar:

- Não exclua a UO de segurança: a unidade organizacional originalmente chamada Segurança durante a configuração da zona de pouso pelo AWS Control Tower não deve ser excluída. Se você excluí-la, verá uma mensagem de erro instruindo a redefinir a zona de pouso imediatamente. Você não poderá executar nenhuma outra ação no AWS Control Tower até que a redefinição seja concluída.
- Não exclua as funções obrigatórias: o AWS Control Tower verifica determinadas funções AWS Identity and Access Management (IAM) quando você faz login no console para verificar a variação de funções do IAM. Se esses perfis estiverem ausentes ou inacessíveis, será exibida uma página de erro instruindo que é necessário redefinir a zona de pouso. Esses perfis são `AWSControlTowerAdmin`, `AWSControlTowerCloudTrailRole` e `AWSControlTowerStackSetRole`.

  Para obter mais informações sobre esses perfis, consulte Permissões obrigatórias para usar o console do AWS Control Tower.
- Não exclua todos os adicionais OUs: 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 desvio, mas você ainda poderá usar o AWS Control Tower. Pelo menos uma UO adicional é necessária para que o AWS Control Tower opere, mas não precisa ser a UO Sandbox.
- Não remova contas compartilhadas: se você remover contas compartilhadas do Foundational OUs, como remover a conta de registro da OU de segurança, sua landing zone ficará em um estado de desvio. A zona de pouso deve ser redefinida para que você possa continuar usando o console do AWS Control Tower.

Alterações reparáveis em recursos

Veja a seguir uma lista de alterações nos recursos do AWS Control Tower que são permitidas, embora elas criem um desvio reparável. Os resultados dessas operações permitidas podem ser visualizados no console do AWS Control Tower, embora uma atualização possa ser necessária.

Consulte mais informações sobre como resolver o desvio resultante em Managing Resources Outside of AWS Control Tower.

Alterações permitidas fora do console do AWS Control Tower

- Altere o nome de uma OU registrada.
- Altere o nome da UO de segurança.
- Altere o nome das contas dos membros em Não fundacional OUs.
- Altere o nome das contas compartilhadas do AWS Control Tower na UO de segurança.
- Exclua uma UO não fundamental.
- Exclua uma conta inscrita de uma UO não fundamental.
- 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.

Drift e provisionamento de novas contas

Se a zona de pouso estiver em um estado de desvio, o recurso Inscrever conta no AWS Control Tower não funcionará. Nesse caso, é necessário provisionar contas no AWS Service Catalog. Para obter instruções, consulte Provisionar contas com AWS Service Catalog Account Factory .

Em específico, se você fez certas alterações nas contas pelo Service Catalog, como alterar o nome do portfólio, recurso Inscrever conta não funcionará.

Tipos de deriva de governança

O desvio de governança, também chamado de desvio organizacional, ocorre quando OUs SCPs, e as contas dos membros são alteradas ou atualizadas. Tipos de desvio de governança que podem ser detectados no AWS Control Tower:

- Conta de membro movida

- Conta de membro removida
- Atualização não planejada do SCP gerenciado
- SCP anexado à conta do membro
- SCP conectado à OU gerenciada
- SCP separado da OU gerenciada

Outro tipo é o desvio da zona de pouso, que pode ser encontrado na conta de gerenciamento. A variação da zona de destino consiste na mudança de função do IAM ou em qualquer tipo de mudança organizacional que afete especificamente as contas básicas OUs e compartilhadas.

- UO fundamental excluída
- Acesso confiável desabilitado

Um caso especial de desvio da zona de pouso é o desvio de perfil, que é detectado quando um perfil necessário não está disponível. Se esse tipo de desvio ocorrer, o console exibirá uma página de aviso e algumas instruções sobre como restaurar o perfil. A zona de pouso não estará disponível até que a mudança de perfil seja resolvida. Consulte mais informações sobre o desvio em Não exclua os perfis necessários na seção chamada Tipos de desvio a serem resolvidos imediatamente.

O AWS Control Tower relata desvios de controle em relação aos controles implementados com políticas de controle de recursos (RCPs) e aos controles que fazem parte do padrão AWS Security Hub gerenciado por serviços: AWS Control Tower.

- Desvio de controle do Security Hub
- Derivação da política de controle

O AWS 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.

Conta de membro movida

Esse tipo de desvio ocorre na conta e não na UO. Esse tipo de desvio pode ocorrer quando uma conta-membro do AWS Control Tower, a conta de auditoria ou a conta de arquivamento de logs é

transferida de uma UO registrada do AWS Control Tower para qualquer outra UO. Veja um exemplo da notificação do Amazon SNS 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 UO com até mil contas, você pode resolvê-lo da seguinte maneira:

- Acesse a página Organização no console do AWS Control Tower, selecione a conta e Atualizar conta no canto superior direito (opção mais rápida para contas individuais).
- Acesse a página Organização no console do AWS Control Tower e escolha Inscrever novamente na UO que contém a conta (opção mais rápida para várias contas). Para obter mais informações, consulte Registrar uma unidade organizacional existente com o 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: Provisionar e atualizar contas usando automação.

- Quando esse tipo de desvio ocorre em uma UO com mais de mil contas, a resolução do desvio pode depender do tipo de conta que foi movida, conforme explicado nos próximos parágrafos. Para obter mais informações, consulte Atualizar a zona de pouso.
  - Se uma conta provisionada pelo Account Factory for movida: em uma UO com menos de mil contas, você pode resolver o desvio da conta atualizando o produto provisionado no Account Factory, registrando novamente a UO ou atualizando a zona de pouso.

    Em uma OU com mais de 1.000 contas, você deve resolver o problema fazendo uma atualização em cada conta transferida, seja por meio do console do AWS Control Tower ou do produto provisionado, pois o registro novo 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 é movida: é possível resolver o desvio ao mover a conta de auditoria ou de arquivamento de logs atualizando a zona de pouso. Para obter mais informações, consulte Atualizar a zona de pouso.

⚠ Nome de campo desativado

O nome do campo `MasterAccountID` foi alterado `ManagementAccountID` para estar em conformidade com AWS as diretrizes. O nome antigo foi desativado. Desde 2022, os scripts que contêm o nome do campo obsoleto não funcionam mais.

Conta de membro removida

Esse tipo de desvio pode ocorrer quando uma conta-membro é removida de uma unidade organizacional registrada do AWS Control Tower. O exemplo a seguir mostra a notificação do Amazon SNS 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-membro, você pode resolvê-lo atualizando a conta no console do AWS Control Tower ou no Account Factory. Por exemplo, você pode adicionar a conta a outra UO registrada pelo 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 UO fundamental, você deverá resolver o desvio redefinindo a zona de pouso. Até que esse desvio seja resolvido, você não poderá usar o console do AWS Control Tower.
- Para obter mais informações sobre como resolver o desvio de contas e OUs, consulte. Se você gerencia recursos fora do AWS Control Tower

> **Note**
>
> No Service Catalog, o produto provisionado do Account Factory que representa a conta não é atualizado para removê-la. 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 selecione Encerrar.

Atualização não planejada do SCP gerenciado

Esse tipo de desvio pode ocorrer quando um SCP para um controle é atualizado no AWS Organizations console ou programaticamente usando o AWS AWS CLI ou um deles. SDKs Veja um exemplo da notificação do Amazon SNS 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

Para resolver esse tipo de desvio quando ele ocorre em uma UO com até mil contas:

- Acesse a página Organização no console do AWS Control Tower para registrar novamente a UO (opção mais rápida). Para obter mais informações, consulte Registrar uma unidade organizacional existente com o AWS Control Tower.
- Atualização da zona de pouso (opção mais lenta). Para obter mais informações, consulte Atualizar a zona de pouso.

Quando esse tipo de desvio ocorre em uma UO com mais de mil contas, resolva-o atualizando a zona de pouso. Para obter mais informações, consulte Atualizar a zona de pouso.

SCP conectado à OU gerenciada

Esse tipo de desvio pode ocorrer quando uma SCP para um controle é anexada a qualquer outra UO. Essa ocorrência é especialmente comum quando você está trabalhando em você OUs de fora do console do AWS Control Tower. Veja um exemplo da notificação do Amazon SNS 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

Para resolver esse tipo de desvio quando ele ocorre em uma UO com até mil contas:

- Acesse a página Organização no console do AWS Control Tower para registrar novamente a UO (opção mais rápida). Para obter mais informações, consulte Registrar uma unidade organizacional existente com o AWS Control Tower.
- Atualização da zona de pouso (opção mais lenta). Para obter mais informações, consulte Atualizar a zona de pouso.

Quando esse tipo de desvio ocorre em uma UO com mais de mil contas, resolva-o atualizando a zona de pouso. Para obter mais informações, consulte Atualizar a zona de pouso.

SCP separado da OU gerenciada

Esse tipo de desvio pode ocorrer quando uma SCP de um controle é separada de uma UO gerenciada pelo AWS Control Tower. Essa ocorrência é especialmente comum quando você está trabalhando fora do console do AWS Control Tower. Veja um exemplo da notificação do Amazon SNS 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

Para resolver esse tipo de desvio quando ele ocorre em uma UO com até mil contas:

- Acesse a UO no console do AWS Control Tower para registrar a UO novamente (opção mais rápida). Para obter mais informações, consulte Registrar uma unidade organizacional existente com o AWS Control Tower.
- Atualização da zona de pouso (opção mais lenta). Se o desvio estiver afetando um controle obrigatório, o processo de atualização cria uma política de controle de serviços (SCP) e a anexa à UO para resolvê-lo. Consulte mais informações sobre como atualizar a zona de pouso em Atualizar a zona de pouso.

Quando esse tipo de desvio ocorre em uma UO com mais de mil contas, resolva-o atualizando a zona de pouso. Se o desvio estiver afetando um controle obrigatório, o processo de atualização cria uma política de controle de serviços (SCP) e a anexa à UO para resolvê-lo. Consulte mais informações sobre como atualizar a zona de pouso em Atualizar a zona de pouso.

SCP anexado à conta do membro

Esse tipo de desvio pode ocorrer quando uma SCP é anexada a uma conta no console do 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 do AWS Control Tower. Veja um exemplo da notificação do Amazon SNS 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 UO.

Quando esse tipo de desvio ocorre para contas em uma UO fundamental, como a UO de segurança, a solução é atualizar a zona de pouso. Para obter mais informações, consulte Atualizar a zona de pouso.

Para resolver esse tipo de desvio quando ele ocorre em uma UO não fundamental com até mil contas:

- Desanexe a SCP do AWS Control Tower da conta do Account Factory.
- Acesse a UO no console do AWS Control Tower para registrar a UO novamente (opção mais rápida). Para obter mais informações, consulte Registrar uma unidade organizacional existente com o AWS Control Tower.

Quando esse tipo de desvio ocorre em uma UO com mais de mil contas, você pode tentar resolvê-lo atualizando a configuração da conta do Account Factory. Talvez não seja possível resolvê-lo com sucesso. Para obter mais informações, consulte Atualizar a zona de pouso.

UO fundamental excluída

Esse tipo de desvio se aplica somente ao AWS Control Tower Foundational OUs, como a Security OU. Isso poderá ocorrer se uma UO fundamental 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 a zona de pouso, o AWS Control Tower substitui a UO fundamental no local original. O exemplo a seguir mostra uma notificação do Amazon SNS que você pode receber quando esse tipo de desvio é 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 e OUs, 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 padrão gerenciado pelo serviço do AWS Security Hub : o AWS Control Tower relata um estado de desvio. O serviço do AWS Security Hub em si não relata um estado de desvio para esses controles. Em vez disso, o serviço envia suas descobertas ao AWS Control Tower.

O desvio de controle do Security Hub também poderá ser detectado se o 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, o AWS Control Tower verifica se o controle está em desvio. O exemplo a seguir mostra uma notificação do Amazon SNS que você pode receber quando esse tipo de desvio é 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" : "SH.XXXXXXX.1",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
```

```
"EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>".
"Region" : "us-east-1"
}
```

Resolução

Para OUs com menos de 1000 contas, a resolução recomendada é chamar a ResetEnabledControlAPI para o controle derivado. No console, você pode selecionar Registrar novamente para a OU, o que redefine o controle para o estado original. Como alternativa, para qualquer OU, você pode remover e reativar o controle por meio do console ou do AWS Control Tower APIs, que também redefine o controle.

Para obter mais informações sobre como resolver o desvio de contas e OUs, consulte. Se você gerencia recursos fora do AWS Control Tower

Derivação da política de controle

Esse tipo de desvio ocorre quando um controle implementado com políticas de controle de recursos (RCPs) ou políticas declarativas relata um estado de desvio. Ele retorna um estado de`CONTROL_INEFFECTIVE`, que você pode ver no console do AWS Control Tower e na mensagem de deriva. A mensagem de desvio para esse tipo de desvio também inclui a mensagem `EnabledControlIdentifier` para o controle afetado.

Esse tipo de desvio não é relatado para controles baseados em SCP.

O exemplo a seguir mostra uma notificação do Amazon SNS que você pode receber quando esse tipo de desvio é detectado.

```
{
    "Message": "AWS Control Tower detects that a policy it owns was updated
 unexpectedly. This mismatch indicates that configuration changes were made outside of
 AWS Control Tower.",
    "MasterAccountId": "123456789XXX",
    "ManagementAccountId": "123456789XXX",
    "OrganizationId": "o-123EXAMPLE",
    "DriftType": "CONTROL_INEFFECTIVE",
    "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if
 permitted or Re-register the OU. If the problem persists, contact AWS support.",
    "TargetIdentifier": "arn:aws:::organizations/o-123456/ou-1234-4567",
    "ControlId": "CT.XXXXXXX.PV.1",
    "ControlName": "EBS snapshots should not be publicly restorable",
```

```
    "ApiControlIdentifier": "arn:aws:controlcatalog:::control/<UNIQUE_ID>",
    "EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>"
}
```

Resolução

A solução mais fácil para o desvio da política de controle em controles RCP, controles de política declarativa e controles do Security Hub habilitados no AWS Control Tower é chamar a API. `ResetEnabledControl`

Para OUs com menos de 1000 contas, outra solução do console ou da API é registrar novamente a OU, o que redefine o controle para o estado original.

Para qualquer OU individual, você pode remover e reativar o controle por meio do console ou do AWS Control Tower APIs, que também redefine o controle.

Para obter mais informações sobre como resolver o desvio de contas e OUs, consulte. Se você gerencia recursos fora do AWS Control Tower

Acesso confiável desabilitado

Esse tipo de desvio se aplica às zonas de pouso do AWS Control Tower. Isso ocorre quando você desativa o acesso confiável ao AWS Control Tower AWS Organizations depois de configurar sua zona de pouso do AWS Control Tower.

Quando o acesso confiável é desabilitado, o AWS Control Tower não recebe mais eventos de alteração do AWS Organizations. O AWS Control Tower depende desses eventos de mudança para se manter sincronizado com eles. AWS Organizations Como resultado, o AWS Control Tower pode perder mudanças organizacionais nas contas OUs e. É por isso que é importante registrar novamente cada UO, sempre que você atualizar a zona de pouso.

Exemplo: notificação do Amazon SNS

Veja a seguir um exemplo da notificação do Amazon SNS 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

O AWS Control Tower notifica você quando esse tipo de desvio ocorre no console do AWS Control Tower. A solução é redefinir a zona de pouso do AWS Control Tower. Consulte mais informações em Resolving drift.

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. É possível alterar esses recursos dentro do AWS Control Tower ou fora dele. O local mais comum para alterar recursos fora do AWS Control Tower é o console do AWS Organizations . Este tópico descreve como reconciliar alterações em recursos do AWS Control Tower ao fazer as alterações fora do AWS Control Tower.

Renomear, excluir e mover recursos fora do console do AWS Control Tower pode fazer com que o console fique dessincronizado. Muitas alterações podem ser reconciliadas automaticamente. Certas alterações exigem um reparo na zona de pouso para atualizar as informações exibidas no console do AWS Control Tower.

Em geral, as alterações feitas fora do console do AWS Control Tower nos recursos do AWS Control Tower criam um estado de desvio reparável na zona de pouso. Consulte mais informações sobre essas alterações em Alterações reparáveis em recursos.

Tarefas que exigem redefinição da zona de pouso

- Excluir a UO de segurança (um caso especial, não deve ser feito sem motivo).
- Remover uma conta compartilhada da UO de segurança (não recomendado).
- Atualizar, anexar ou desanexar uma SCP associada à UO 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

- Criar uma unidade organizacional (UO) de nível superior
- Renomear uma UO registrada
- Excluir uma UO registrada (exceto a UO de segurança, que requer uma atualização).
- Excluir 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 ao conciliar suas mudanças. Para obter mais informações sobre a atualização de um produto provisionado, consulte Atualização de produtos provisionados na documentação. AWS Service Catalog

Referir-se a recursos fora do AWS Control Tower

Quando você cria contas novas OUs e 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. Elas são exibidas na página Organização, mas não são administrados pelos controles do AWS Control Tower.

Criar uma conta

Contas criadas fora do AWS Control Tower são chamadas de Não inscritas. As contas inscritas e não inscritas que pertencem a uma UO registrada no AWS Control Tower são exibidas na página Organização. Contas que não pertencem a uma UO registrada podem ser convidadas usando o console do AWS Organizations . Esse convite para participar não inscreve a conta no AWS Control Tower nem estende a governança do AWS Control Tower para a conta. Para estender a governança inscrevendo a conta, acesse a página Organização na página Detalhe da conta no AWS Control Tower e selecione 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 UO fora do AWS Control Tower, ele reflete automaticamente a alteração do nome. No entanto, se você provisionar suas contas usando o AWS Service Catalog, você também deverá redefinir a zona de pouso para garantir que o AWS Control Tower permaneça consistente com o AWS Organizations. O fluxo de trabalho de redefinição garante a consistência entre os serviços básicos e adicionais OUs. É possível resolver esse tipo de desvio na página Configurações de zona inicial. Consulte a seção chamada “Resolver desvios” em Detectar e resolver desvios no AWS Control Tower.

O AWS Control Tower exibe os nomes da OUs 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 Gerenciamento de Faturamento e Custos da AWS 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.

Excluir a UO de segurança

Esse tipo de oscilação é um caso especial. Se excluir a UO de segurança será exibida uma página de mensagem de erro solicitando redefinir a zona de pouso. É necessário redefinir a zona de pouso antes de poder executar 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 poderá visualizar a página Configurações de zona inicial para localizar o botão Redefinir.

Nessa situação, o processo de redefinição da zona de pouso cria outra UO de segurança e move as duas contas compartilhadas para a nova UO de segurança. O AWS Control Tower marca as contas de arquivamento de logs e de auditoria como com desvio. O mesmo processo resolve o desvio nessas contas.

Se você determinar que deve excluir a UO de segurança, saiba que:

Antes de excluir a UO de segurança, é necessário verificar se ela não contém contas. Especificamente, é necessário remover as contas de arquivamento de logs e de auditoria da UO. Recomendamos que você mova essas contas para outra UO.

> **Note**
>
> A ação de excluir a UO de segurança não deve ser executada sem a devida consideração. A ação poderá criar preocupações de conformidade se o registro em log for suspenso temporariamente e porque alguns controles poderão não ser aplicados.

Para obter informações gerais sobre oscilação, consulte "Resolver oscilações" em Detectar e resolver desvios no AWS Control Tower.

Remover uma conta da OU de segurança

Não recomendamos que você remova nenhuma das contas compartilhadas da sua organização nem as retire da UO de segurança. Se você tiver removido uma conta compartilhada por engano, poderá seguir os passos de correção nesta seção para restaurar a conta.

- No console do AWS Control Tower: para iniciar o processo de correção, siga as etapas semimanuais. Certifique-se de que o usuário ou o perfil que você usa para acessar o console do AWS Control Tower tenha permissões para executar `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 do AWS Control Tower, você precisará de um usuário ou perfil com a política gerenciada `AWSControlTowerServiceRolePolicy` ou equivalente e permissão para executar todas as ações do AWS Control Tower (controltower:*).
- Se as etapas de correção não restaurarem a conta, entre em contato com o 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 serviço (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 faz mais parte da organização. Resultado: as atualizações e redefinições do AWS Control Tower falharão.

Para restaurar uma conta compartilhada usando o console do AWS Control Tower (procedimento semimanual)

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 Centro de Identidade do IAM ou perfil 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 Desvio da zona de pouso detectado, escolha Convidar novamente para corrigir a remoção da conta compartilhada, convidando-a novamente para a organização. Um e-mail gerado automaticamente é enviado ao endereço de e-mail da conta.
3. Aceite o convite para trazer a conta compartilhada de volta à 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 acessar diretamente 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 Desvio da zona de pouso. Escolha Redefinir para reparar a zona de pouso.
5. Aguarde a conclusão do processo de redefinição.

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 o 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 Centro de Identidade do IAM ou perfil com a política gerenciada `AWSOrganizationsFullAccess` ou equivalente.
2. Convide a conta compartilhada de volta à 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 do novamente.
5. Faça login no console do AWS Control Tower como usuário ou perfil com a política gerenciada `AWSControlTowerServiceRolePolicy` ou equivalente e permissões para executar todas as ações do AWS Control Tower (controltower:*).
6. Você verá a página Desvio da zona de pouso com a opção de redefinir a zona de pouso. Escolha Redefinir para reparar a zona de pouso.
7. Aguarde a conclusão do processo de redefinição.

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 o AWS Support.

Alterações externas que são atualizadas automaticamente

As alterações feitas nos endereços de e-mail da sua conta são atualizadas pelo AWS Control Tower automaticamente, 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 de contas compartilhadas e de outras contas são atualizados e exibidos de forma consistente no AWS Control Tower depois de alterá-los.

> **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.

Excluir recursos do AWS Control Tower fora do AWS Control Tower

Você pode excluir OUs contas no AWS Control Tower e não precisa realizar nenhuma outra ação para ver as atualizações. O Account Factory é atualizado automaticamente quando você exclui uma UO, mas não quando você exclui uma conta.

Excluir uma UO registrada (exceto a UO de segurança)

Dentro AWS Organizations, você pode remover unidades organizacionais vazias (OUs) usando a API ou o console. OUs 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 cadastrados OUs permaneça consistente.

> **Note**
>
> Em AWS Service Catalog, o Account Factory é atualizado para remover a OU excluída da lista de disponíveis OUs na qual você pode provisionar uma conta.

Excluir uma conta registrada de uma UO

Quando você exclui uma conta inscrita, 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).

Administrar organizações e contas com o 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 tem 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 inscrever contas individualmente. Consulte mais informações sobre como inscrever contas individuais em Inscrever um existente Conta da AWS.

Terminologia

- Quando você traz uma organização existente para o AWS Control Tower, isso se chama registrar a organização ou estender a governança à organização.
- Quando você traz uma AWS conta para o AWS Control Tower, isso se chama cadastrar a conta.

Visualize OUs suas contas

Na página da AWS Control Tower Organization, você pode ver todas as suas AWS Organizations, incluindo OUs aquelas registradas OUs na AWS Control Tower e aquelas 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 da organização, independentemente da UO ou do status de inscrição no AWS Control Tower. Uma maneira fácil de visualizar suas contas na página Organização é selecionar Somente contas no menu suspenso no canto superior direito. Você pode visualizar, atualizar e inscrever contas individualmente no OUs, 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 seus recursos do AWS Control Tower. Consulte mais informações sobre a página Organização na demonstração em vídeo.

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.

Demonstração em vídeo sobre como trabalhar com a página Organização no AWS Control Tower.

Tópicos

- Registrar uma unidade organizacional existente com o AWS Control Tower
- Inscrever um existente Conta da AWS

Estender a governança a uma organização existente

É possível adicionar a governança do AWS Control Tower a uma organização existente configurando uma zona de pouso (LZ) conforme descrito no Guia do usuário do em Getting Started, Step 2.

Veja o que esperar ao configurar a zona de pouso do AWS Control Tower em uma organização existente.

- Você pode ter uma landing zone por AWS Organizations organização.
- O AWS Control Tower usa a conta de gerenciamento da sua AWS Organizations organização atual como sua conta de gerenciamento. Nenhuma nova conta de gerenciamento é necessária.
- No entanto, o AWS Control Tower configura duas novas contas em uma UO registrada: uma conta de auditoria e uma conta de arquivamento de logs.
- Os limites de serviço da sua organização devem permitir a criação dessas duas contas adicionais.
- Depois de iniciar a zona de pouso ou registrar uma UO, os controles do AWS Control Tower se aplicam automaticamente a todas as contas inscritas nessa UO.
- Você pode inscrever outras AWS contas existentes em uma OU que seja governada pelo AWS Control Tower, para que os controles se apliquem a essas contas.
- Você pode adicionar mais OUs no AWS Control Tower e registrar os existentes OUs.

Consulte outros pré-requisitos de registro e inscrição em Getting Started with AWS Control Tower.

Aqui estão mais detalhes sobre como os controles do AWS Control Tower não se aplicam às suas OUs organizações da AWS que não têm zonas de pouso da AWS Control Tower configuradas:

- As novas contas criadas fora do Account Factory do AWS Control Tower não são limitadas pelos controles da UO registrada.
- Novas contas criadas OUs que não estão registradas no AWS Control Tower não estão vinculadas a controles, a menos que você inscreva especificamente essas contas no 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 inscreva a conta.

Para obter mais informações sobre como aplicar o AWS Control Tower às contas existentes OUs e às contas, consulteRegistrar uma unidade organizacional existente com o AWS Control Tower.

Consulte uma visão geral do processo de configuração de uma zona de pouso do AWS Control Tower em sua organização existente no vídeo na próxima seção.

> **Note**
>
> Durante a configuração, o AWS Control Tower realiza verificações prévias 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 o AWS Control Tower em sua organização para determinar se o AWS Control Tower pode interferir na implantação atual da sua zona de pouso. Além disso, consulte informações sobre como mover contas de um zona de pouso para outra em Se a conta não atender aos pré-requisitos.

Vídeo: habilitar uma zona de pouso no AWS Organizations existente

Este vídeo (7:48) descreve como configurar e habilitar uma zona de pouso do 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.

Enable AWS Control Tower for existing organizations

Considerações sobre o Centro de Identidade do IAM e as organizações existentes

- Se o AWS IAM Identity Center (IAM Identity Center) já estiver configurado, a região de origem do AWS Control Tower deverá ser a mesma que a região do IAM Identity Center.
- O AWS Control Tower não exclui uma configuração existente.
- Se o Centro de Identidade do IAM já estiver habilitado e você estiver usando o Diretório do Centro de Identidade do IAM, 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) for configurado, o AWS Control Tower não alterará a configuração existente. Consulte mais detalhes em Considerações para clientes AWS IAM Identity Center (IAM Identity Center).

Acesso a outros AWS serviços

Depois de incluir sua organização na governança do AWS Control Tower, você ainda terá acesso a todos os AWS serviços que estão disponíveis por meio do AWS Organizations console APIs e. AWS Organizations Para obter mais informações, consulte Serviços relacionados da AWS.

Aninhado OUs na AWS Control Tower

Este capítulo lista as expectativas e considerações que você deve conhecer ao trabalhar com o nested OUs in AWS Control Tower. Na maioria das formas, trabalhar com aninhado OUs é o mesmo que trabalhar com uma estrutura de OU plana. Os recursos de Registro e Registro Novo funcionam com o nested OUs, exceto pelos comportamentos alterados que são observados neste capítulo.

Vídeo de demonstração

Este vídeo (4:46) descreve como gerenciar implantações de UOs 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.

Passo a passo em vídeo do gerenciamento do Nested OUs no AWS Control Tower.

Para obter orientação sobre as melhores práticas para o nested OUs e sua zona de pouso, consulte a postagem do blog Organizing your AWS Control Tower landing zone with OUs nested.

Expandir de uma estrutura de UO plana para uma estrutura de UO aninhada

Se você criou a zona de pouso do AWS Control Tower com uma estrutura de UO plana, é possível expandi-la para uma estrutura de UO aninhada.

Esse processo tem quatro etapas principais:

1. Crie a estrutura de UO 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 UO da qual você deseja mover contas.
   b. Selecione todas as contas da UO.
   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 UO aninhada no AWS Control Tower e opte pelo Registro ou Novo registro dela. Todas as contas na UO aninhada serão inscritas.
   - Se você criou a UO no AWS Control Tower, opte pelo Novo registro dela.
   - 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 UO aninhada

Para apoiar o registro bem-sucedido de suas contas aninhadas OUs e de seus membros, o AWS Control Tower realiza uma série de pré-verificações. Essas mesmas pré-verificações são realizadas ao registrar qualquer UO de nível superior ou UO aninhada. Consulte mais informações em Common causes of failure during registration or re-registration.

- Se todas as pré-verificações forem aprovadas, o AWS Control Tower começará o registro da UO automaticamente.

- Se alguma pré-verificação falhar, o AWS Control Tower interromperá o processo de registro e fornecerá uma lista de itens que devem ser corrigidos antes que você possa registrar a UO.

Aninhado OUs e funções

O AWS Control Tower implanta a `AWSControlTowerExecution` função em contas na OU de destino e em todas as contas OUs aninhadas na OU de destino, mesmo quando sua intenção é registrar somente a OU de destino. Esse perfil concede a qualquer usuário da conta de gerenciamento permissões de Administrador em qualquer conta que tenha o perfil `AWSControlTowerExecution`. O perfil pode ser usado para realizar ações que normalmente não seriam permitidas pelos controles do AWS Control Tower.

Você pode excluir esse perfil de contas não inscritas que não planeja inscrever. Se você excluir essa função, não poderá registrar a conta no AWS Control Tower nem registrar o responsável imediato OUs, a menos que você restaure a função na conta. Para excluir o perfil `AWSControlTowerExecution` de uma conta, é necessário fazer login com o perfil `AWSControlTowerExecution`, porque nenhuma outra entidade principal do IAM tem permissão para excluir perfis gerenciados pelo AWS Control Tower.

Consulte informações sobre como restringir o acesso ao perfil Optional conditions for your role trust relationships.

O que acontece durante o registro e o novo registro de contas aninhadas OUs

Quando você faz o registro ou o novo registro de uma UO aninhada, o AWS Control Tower inscreve todas as contas não inscritas da UO de destino e atualiza todas as contas inscritas. Veja o que esperar:

O AWS Control Tower realiza as seguintes tarefas

- Adiciona a `AWSControlTowerExecution` função a todas as contas não inscritas nesta OU e a todas as contas não inscritas em sua lista aninhada. OUs
- Registra contas-membros que não estão inscritas.
- Reinscreve as contas-membros inscritas.
- Cria um login do Centro de Identidade do IAM para contas-membros recém-inscritas.
- Atualiza as contas-membros inscritas existentes para refletir as mudanças na zona de pouso.

- Atualiza os controles que estão configurados para essa UO e suas contas-membros.

Considerações sobre o registro de UO aninhada

- Não é possível registrar uma UO na UO principal (UO de segurança).
- O Nested OUs deve ser registrado separadamente.
- Não é possível registrar uma UO a menos que a UO principal esteja registrada.
- Você não pode registrar uma OU a menos que todas as partes OUs superiores da árvore tenham sido registradas com sucesso em algum momento (algumas podem ter sido excluídas).
- É possível registrar uma UO que esteja sob uma UO derivada superior, mas o desvio não é reparado por essa ação.

Limitações da UO aninhada

- OUs pode ser aninhado a no máximo 5 níveis de profundidade abaixo da raiz.
- Aninhado OUs sob a OU de destino, deve ser registrado ou registrado novamente separadamente.
- Se a UO de destino estiver no Nível 2 ou abaixo na hierarquia, ou seja, se não for uma UO de nível superior, os controles preventivos ativados em níveis superiores OUs serão aplicados automaticamente nessa OU e em todas as que estão OUs abaixo dela.
- As falhas de registro da UO não se propagam na árvore hierárquica. Você pode ver detalhes sobre os estados de aninhado OUs na página de detalhes da OU dos pais.
- As falhas de registro da UO não se propagam pela árvore hierárquica.
- O AWS Control Tower não modifica as configurações da VPC para nenhuma conta nova ou existente.

Aninhado OUs e em conformidade

No console do AWS Control Tower, você pode ver OUs todas as contas que não estão em conformidade na página Organização, para que você possa entender a conformidade em uma escala maior.

Considerações sobre conformidade para contas aninhadas OUs e

- A conformidade de uma OU não é determinada com base na conformidade do OUs aninhado abaixo dela.

- O status de conformidade de um controle é calculado OUs em todas as áreas nas quais o controle está ativado, inclusive OUs aninhado. Veja o status de conformidade OUs e as contas do AWS Control Tower.
- Uma UO é mostrada como não estando em conformidade somente se tiver contas que não estejam em conformidade, independentemente de onde a UO esteja na hierarquia da UO.
- Se uma UO aninhada não estiver em conformidade, a UO principal não será automaticamente considerada como não estando em conformidade.
- 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 sua conta OUs ou suas contas mostrem um status de não conformidade.

Aninhado OUs e à deriva

Em determinadas situações, a deriva pode impedir o registro de OUs aninhados.

Expectativas de deriva e aninhamento OUs

- Você pode ativar os controles ativados OUs com pais desviados, mas não diretamente com os pais desviados OUs.
- Você tem permissão para habilitar os controles de detecção em uma UO com desvio, desde que não seja uma UO com desvio de nível superior.
- Os controles obrigatórios são ativados OUs somente no nível superior. Os controles obrigatórios são ignorados quando você registra uma UO aninhada.
- Um controle obrigatório protege AWS Config os recursos; portanto, esse controle deve estar em um estado não desviado para se registrar aninhado. OUs Se for desviado, o AWS Control Tower bloqueia o registro de aninhados OUs.
- 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.

Aninhado OUs e controles

Quando você habilita um controle em uma UO registrada, os controles preventivos e de detecção têm comportamentos diferentes. Para controles aninhados OUs e proativos, o comportamento é semelhante aos controles de detetive.

Controles preventivos

- Os controles preventivos são aplicados no OUs nested.
- Os controles preventivos obrigatórios são aplicados em todas as contas da OU e suas contas OUs aninhadas.
- Os controles preventivos afetam todas as contas e estão OUs aninhados na OU de destino, mesmo que essas contas não OUs estejam registradas.

Controles proativos e de detecção

- O Nested OUs não herda controles de detetive ou proativos automaticamente; eles devem ser ativados separadamente.
- Controles proativos e de detecção são implantados somente em contas registradas nas regiões operacionais da zona de pouso.

Estados de controle e herança habilitados

É possível ver os controles herdados de cada UO na página Detalhes da UO.

> **Tip**
>
> É possível usar a herança de controle para ajudar a permanecer dentro da cota de SCP de uma UO. Por exemplo, é possível habilitar um controle na UO de nível superior de uma hierarquia de UO, em vez de habilitar diretamente para uma UO aninhada.

Status herdado

- O status Herdado indica que o controle é habilitado somente por herança e não foi aplicado diretamente à UO.
- O status Ativado significa que o controle é aplicado nesta OU, independentemente de seu estado em outra OUs.
- O status Falha significa que o controle não é aplicado nesta OU, independentemente de seu estado em outra OUs.

> **Note**
>
> O status Herdado indica que o controle foi aplicado a uma UO mais alta na árvore, mas não foi adicionado diretamente a essa UO.

> **Se a zona de pouso não for a versão atual**
>
> Cada linha na tabela Controles habilitados representa um controle habilitado em uma UO individual.

Aninhado OUs e a raiz

A raiz não é uma UO e não é possível fazer seu registro ou novo registro. Também não é possível criar contas diretamente na raiz. A raiz não pode não estar em conformidade nem ter um estado de ciclo de vida, como registrada ou em desvio.

No entanto, a raiz é o contêiner de nível superior para todas as contas e. OUs No contexto de aninhado OUs, é o nó sob o qual todos os outros OUs estão aninhados.

Registrar uma unidade organizacional existente com o AWS Control Tower

Uma forma eficiente de trazer várias AWS contas existentes para a 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 UO contiver mais de mil contas, você não poderá registrá-la no AWS Control Tower.

Quando você registra uma UO, suas contas-membros são inscritas na zona de pouso do AWS Control Tower. Elas são administradas pelos controles que se aplicam à sua UO.

> **Note**
>
> Se você ainda não tem uma zona de pouso do 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. Consulte mais detalhes sobre como configurar um zona de pouso em Conceitos básicos do AWS Control Tower.

O que acontece com minhas contas quando eu registro minha UO?

O AWS Control Tower exige permissão para estabelecer um acesso confiável entre AWS CloudFormation e AWS Organizations em seu nome, para que AWS CloudFormation você possa implantar sua pilha nas contas da sua organização automaticamente.

- O perfil `AWSControlTowerExecution` é adicionado a todas as contas com o status Não inscrita.
- Os controles obrigatórios são habilitados por padrão para sua UO e todas as contas quando você registra sua UO.

Inscrição parcial de contas após o registro de uma UO

É possível registrar uma UO com sucesso, mas algumas contas podem permanecer não inscritas. 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 UO 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 página da UO, como 4 de 5, no campo contas.

Por exemplo, se você ver 4 de 5, isso significa que sua UO tem 5 contas no total, e 4 delas foram inscritas com sucesso, mas uma conta apresentou falha na inscrição durante o processo de Registrar UO. Você pode escolher Registrar UO novamente para inscrever as contas, depois de verificar se elas atendem aos pré-requisitos de inscrição.

Pré-requisitos do usuário do IAM para registrar uma UO

Sua identidade AWS Identity and Access Management (IAM) (usuário ou função) ou identidade de usuário do IAM 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 usuário do IAM ou da identidade do usuário do Centro de Identidade do IAM ao registrar uma UO.

O portfólio relevante é aquele criado pelo AWS Control Tower, chamado Portfólio do Account Factory do AWS Control Tower. Acesse-o selecionando Service Catalog > Account Factory > Portfólio do Account Factory do AWS Control Tower. Depois, selecione a guia chamada Grupos, perfis e usuários para visualizar sua identidade do IAM ou do Centro de Identidade do IAM. Consulte mais informações sobre como conceder acesso na documentação do AWS Service Catalog.

Registrar uma UO existente

No console do 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 UO contiver mais de mil contas, você não poderá registrá-la no AWS Control Tower.

Para registrar uma OU existente a partir do console

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 Organização.
3. Na página Organização, selecione o botão de opções ao lado da UO que você deseja registrar e selecione Registrar unidade organizacional no menu suspenso Ações no canto superior direito ou, se preferir, selecione o nome da UO para que você possa visualizar a página Detalhes da UO dessa UO.
4. Na página Detalhes da UO, no canto superior direito, você pode selecionar Registrar UO no menu suspenso Ações.

O processo de registro leva no mínimo 10 minutos para estender a governança à UO e até mais dois minutos para cada conta adicional.

Para registrar uma OU existente com APIs

Para registrar uma OU existente no AWS Control Tower APIs, você pode chamar a `EnableBaseline` API com o `AWSControlTowerBaseline` in the `baselineIdentifier` field. Para obter mais informações, consulte Registrar uma OU do AWS Control Tower com APIs only.

Resultados do registro de uma UO existente

Depois de registrar uma UO existente, o perfil `AWSControlTowerExecution` permite que o AWS Control Tower estenda a governança às contas individuais. As barreiras de proteção são aplicadas e as informações sobre as atividades da conta são relatadas às contas de auditoria e registro em log.

Outros resultados incluem o seguinte:

- `AWSControlTowerExecution` permite a auditoria pela conta de auditoria do AWS Control Tower.
- `AWSControlTowerExecution` ajuda a configurar o registro em log da organização, para que todos os logs de cada conta sejam enviados à conta de registro em log.
- `AWSControlTowerExecution`garante que os controles selecionados da AWS Control Tower se apliquem automaticamente a cada conta individual em sua conta OUs, bem como a cada nova conta que você criar na AWS Control Tower.

Para uma UO registrada, é possível fornecer relatórios de conformidade e segurança, com base nos recursos de auditoria e registro em log incorporados pelos controles do AWS Control Tower. Suas equipes de segurança e conformidade podem verificar se todos os requisitos foram atendidos e se houve algum desvio organizacional. Consulte mais informações sobre desvios em Detectar e resolver desvios no AWS Control Tower.

> **Note**
>
> Uma situação incomum pode ocorrer quando o AWS Control Tower OUs e suas contas são exibidas. Se você criou uma conta em uma UO registrada e, posteriormente, transferiu essa conta inscrita para outra UO que não está registrada, especialmente se você usa o AWS Organizations para mover a conta, é possível ver o resultado “1 de 0” contas na página de detalhes da UO. Além disso, você pode ter criado outra conta não inscrita nessa UO não registrada. Se houver uma conta não registrada, o console poderá ler “1 de 1” para a UO. Parece que a conta única (recém-criada) está inscrita, mas na verdade não está. Você deve inscrever a nova conta.

Criar uma UO

Veja como criar uma UO ou uma UO aninhada no AWS Control Tower.

Como criar uma UO no AWS Control Tower.

1. Acesse 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 UO.
4. No menu suspenso OU principal, você pode ver a hierarquia dos registrados. OUs Selecione uma UO principal para a nova UO que você está criando.
5. Escolha Adicionar.

> **Tip**
>
> Para adicionar uma UO aninhada em menos etapas, selecione o nome da UO principal mostrado na tabela na página Organização, visualize a página de UO dessa UO principal e escolha Adicionar uma UO no menu suspenso Ações no canto superior direito. A nova UO é criada automaticamente como uma UO aninhada na UO selecionada.

> **Note**
>
> Se a zona de pouso não estiver atualizada, você verá uma lista plana em vez de uma hierarquia no menu suspenso. Mesmo que sua landing zone inclua unidades aninhadas OUs, 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 o aninhado OUs no AWS Control Tower, consulteAninhado OUs na AWS Control Tower.

Causas comuns de falha durante o registro ou novo registro

Em geral, quando você registra ou registra novamente uma UO, todas as contas dentro dessa UO são inscritas no AWS Control Tower. No entanto, é possível que algumas contas não consigam se inscrever, mesmo que a UO como um todo seja registrada com sucesso. Nesses casos, você deve resolver a falha de pré-verificação relacionada à conta e, depois, tentar reinscrever essa conta ou UO.

Se o registro (ou o novo registro) de uma UO ou de qualquer uma de suas contas-membros falhar, o AWS Control Tower retornará mensagens de erro para as contas-membros afetadas. Você pode visualizar as mensagens de erro na página Detalhes da UO, na qual uma tabela agrega as pré-verificações e as mensagens de erro da conta. Se uma operação de Registrar UO falhar, a tabela mostrará todas as mensagens de erro de todas as contas na UO. Se necessário, você também pode ver as mensagens de erro na página 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 offline. 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 a zona de pouso atual ou atualize-a para a versão mais recente.

Erros na UO

- 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 OU se aplica a todos OUs na sua landing zone do AWS Control Tower. Se você tiver SCPs mais do que a cota permite, você deve excluir ou combinar o. SCPs
- Conflitante SCPs

  As existentes SCPs podem ser aplicadas à OU ou à conta, o que impede que o AWS Control Tower registre a conta. Verifique se a política aplicada SCPs pode impedir que o 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

  O AWS Control Tower limita cada UO a mil contas durante o registro.

Erros na conta

- Pré-verificações evitadas em contas

  Uma SCP existente na UO impede que o AWS Control Tower realize pré-verificações em suas contas-membros da UO. Para resolver essa falha de pré-verificação, atualize ou remova a SCP da UO.
- 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]+`
- Gravador ou canal de entrega do Config habilitado

  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 do AWS Control Tower tenha recursos controlados, antes que você possa inscrever uma conta.
- STS desabilitado

  AWS Security Token Service (AWS STS) pode estar desativado na conta. AWS Os endpoints STS devem ser ativados nas contas de todas as regiões suportadas pelo AWS Control Tower.
- Conflito no Centro de Identidade do IAM

  A região de origem do AWS Control Tower não é a mesma que a região AWS IAM Identity Center (IAM Identity Center). Se o Centro de Identidade do IAM já estiver configurado, a região de origem do AWS Control Tower deverá ser a mesma que a região do Centro de Identidade do IAM.
- Tópico do SNS conflitante

  A conta tem um nome de tópico do Amazon Simple Notification Service (Amazon SNS) que o AWS Control Tower precisa usar. O AWS Control Tower cria recursos (como tópicos do SNS) com nomes específicos. Se esses nomes já tiverem sido usados, a configuração do AWS Control Tower falhará. Essa situação poderá ocorrer se você estiver reutilizando uma conta previamente inscrita no AWS Control Tower.

- Conta suspensa detectada

  Essa conta foi suspensa. Ela não pode ser inscrita no AWS Control Tower. Remova a conta dessa UO e tente novamente.

- Usuário do IAM 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 de inscrição. Por exemplo, a conta pode não ter os perfis e as permissões necessárias para inscrevê-la no AWS Control Tower. As instruções para adicionar um perfil estão disponíveis em Adicionar manualmente o perfil do IAM necessário a uma Conta da AWS existente e inscrevê-la.

Como lembrete, AWS CloudTrail é ativado automaticamente em todas as suas AWS contas quando você as inscreve no AWS Control Tower. 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 (UO) ou atualizar várias contas em uma UO é Registrar novamente a UO.

Quando atualizar a AWS Control Tower OUs e as contas

Ao realizar uma atualização da zona de pouso, você deve atualizar as contas inscritas para aplicar novos controles a essas contas.

- Você pode realizar uma atualização em todas as contas em uma UO 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.
- É possível atualizar uma única conta pelo console do AWS Control Tower ou selecionar a opção Atualizar produto provisionado no AWS Service Catalog. Consulte Atualizar a conta no console.

Atualizar várias contas na mesma UO

Repita essas etapas para cada OU em sua organização do AWS Control Tower, se precisar atualizar todas as suas contas OUs e.

Como atualizar várias contas em uma UO, com uma ação

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 Organização.
3. Na página Organização, escolha qualquer UO para visualizar a página Detalhes da UO.
4. Em Ações no canto superior direito, selecione Registrar UO novamente.

Como alternativa, é possível selecionar qualquer conta que mostre o status Atualização disponível e, depois, escolher Atualizar conta, para quantas contas forem necessárias.

O que acontece durante o novo registro

Quando você registra novamente uma UO:

- 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 UO, o perfil `AWSControlTowerExecution` é adicionado a todas as contas com o status Não inscrita ou Falha na inscrição.
- O AWS Control Tower cria um login único (Centro de Identidade do IAM) para essas novas contas inscritas.
- As contas inscritas são reinscritas no AWS Control Tower.
- 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 zona de pouso.

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 -.

AWSControl TowerExecutionRole Isso StackSet na conta de gerenciamento pode falhar porque a função do AWSControlTowerExecutionIAM 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

É possível atualizar contas individuais do AWS Control Tower no console do AWS Control Tower ou no console do Service Catalog.

Para atualizar uma única conta no console do AWS Control Tower, consulteAtualizar 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 opção ao lado do produto provisionado que 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 Atualizar 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 apresenta uma visão geral resumida desses serviços, inclusive informações de configuração sobre os serviços subjacentes e como eles funcionam no AWS Control Tower.

Para ter mais informações sobre como medir um ambiente bem arquitetado, conheça a AWS Well-Architected Tool. Consulte também Management and Governance Cloud Environment Guide.

Tópicos

AWS Opções de backup disponíveis

AWS O Backup permite que você crie um plano de backup para sua landing zone do AWS Control Tower. Você pode incorporar um fluxo de trabalho de backup e recuperação de dados diretamente na sua landing zone. O plano de backup inclui regras predefinidas, como dias de retenção, frequência de backup e a janela de tempo durante a qual o backup ocorre. Para obter mais informações, consulte AWS Backup e AWS Control Tower.

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 AWS APIs solicitaram serviços de suporte 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. Consulte mais informações em About controls in AWS Control Tower.

Gerenciar 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 a zona de pouso, vários grupos podem ser criados automaticamente para o AWS IAM Identity Center , se você selecionar o IAM como seu provedor de identidades. Esses grupos têm conjuntos de permissões que são políticas de permissões predefinidas do IAM. Os usuários finais também pode usar o IAM para definir o escopo de permissões de usuários do IAM e outras entidades nas contas-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 ao Centro de Identidade do IAM e as permissões de usuários em todas as suas contas da AWS 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.

Executar funções de computação sem servidor com o Lambda

Com AWS Lambda, você pode executar código sem provisionar ou gerenciar servidores. Você pode executar o código em vários tipos de aplicações ou serviços de backend, sem a necessidade de sobrecarga de administração adicional. Quando você carrega seu código, o Lambda pode executar e escalar o código com alta disponibilidade. É possível configurar o código para ser acionado de outros serviços da AWS automaticamente ou chamá-lo diretamente em qualquer aplicação da web ou para dispositivos móveis.

Por exemplo, determinados perfis na conta de auditoria do AWS Control Tower podem ser assumidos 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-membros e convidar contas existentes a se juntarem à 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 (OUs). Consulte mais informações sobre o Organizations em Guia do usuário do AWS Organizations.

O AWS Control Tower usa o seguinte OUs:

- Root — O contêiner principal de todas as contas e de todas as outras OUs em sua landing zone.
- Segurança: essa UO contém a conta de arquivamento de logs, a conta de auditoria e os recursos que elas possuem.
- Sandbox: essa UO é criada quando você configura a zona de pouso. Ela e outras crianças OUs em sua landing zone contêm suas contas de membro. Essas são as contas que os usuários finais acessam ao realizar trabalhos em recursos da AWS .

> **Note**
>
> Você pode adicionar mais OUs em sua landing zone por meio do console do AWS Control Tower na página de unidades organizacionais.

Considerações

OUs criados por meio do AWS Control Tower podem ter controles aplicados a eles. OUs criado fora do AWS Control Tower não pode, por padrão. Você pode, no entanto, registrá-los OUs. Depois de registrar uma UO, você pode aplicar controles a ela e a suas contas. Consulte informações sobre o registro de uma UO Register an existing organizational unit with AWS Control Tower.

Armazenar 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 a zona de pouso, um bucket do Amazon S3 é criado na conta de arquivamento de logs para conter todos os logs em todas as contas na zona de pouso.

Monitorar 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. Consulte mais informações em Security Hub standard.

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 reforçar a conformidade com padrões empresariais organizacionais, gerenciar ciclos de vida de produtos e ajudar os usuários a localizar e inicializar produtos com confiança. Consulte mais informações em Guia do administrador do Service Catalog.

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”. Consulte mais informações em Step 2. Crie o AWS Service Catalog produto.

O AWS Control Tower também pode usar o Service Catalog APIs 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 External do AWS Service Catalog

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, revise Updating existing Terraform Open Source products and provisioned products to the External product type no Guia do administrador do AWS Service Catalog .

Essa alteração afeta as contas existentes que você criou ou inscreveu com a o Account Factory Customization do AWS Control Tower. Para fazer a transição dessas contas para o tipo de produto External, você precisa fazer alterações tanto no AWS Service Catalog quanto no AWS Control Tower.

Como fazer a transição para o tipo de produto External

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 esquemas existentes do Terraform Open Source.
3. No AWS Control Tower, atualize cada conta usando um esquema do Terraform Open Source para usar o novo esquema External.

   a. Para atualizar um esquema, você deve primeiro remover completamente o esquema do Terraform Open Source. Consulte mais detalhes em Remove a blueprint from an account.

   b. Adicione o novo esquema External à mesma conta. Consulte mais detalhes em Add a blueprint to an AWS Control Tower account.
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 o Account Factory Customization do AWS Control Tower devem fazer referência a esquemas usando o tipo de produto AWS CloudFormation ou External.

   Para esquemas criados usando o tipo de produto External, o AWS Control Tower permite apenas personalizações de contas que usam modelos do Terraform e o mecanismo de referência do Terraform. Para saber mais, consulte Set up for customization.

> **Note**
>
> O AWS Control Tower não é compatível com o Terraform Open Source como um tipo de produto ao criar 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 seu representante de conta para solicitar assistência.

Rastrear alertas por meio do Amazon Simple Notification Service

O Amazon Simple Notification Service (Amazon SNS) é um serviço web que permite que aplicações, usuários finais e dispositivos enviem e recebam notificações da nuvem instantaneamente. Consulte mais informações no Guia do desenvolvedor do Amazon Simple Notification Service.

O AWS Control Tower usa o Amazon SNS para enviar alertas programáticos aos endereços de e-mail da conta de gerenciamento e de auditoria. Esses alertas ajudam a evitar desvios na zona de pouso. Para obter mais informações, consulte Detectar e resolver desvios no 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 assinar `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 assinar manualmente, usando e-mail ou qualquer tipo de assinatura que o SNS permita. A instrução `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 no 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 do AWS Control Tower, AWS IAM Identity Center solicite AWS Identity and Access Management (IAM) ou a autenticação de que você é um usuário aprovado. AWS Por exemplo, se estiver usando o console do AWS Control Tower, você autentica sua identidade fornecendo suas credenciais da AWS , conforme fornecido pelo seu administrador.

Depois de autenticar sua identidade, o IAM controla seu acesso AWS com um conjunto definido de permissões em um conjunto específico de operações e recursos. Se você for o administrador da conta, poderá usar o IAM para controlar o acesso de outros usuários do IAM aos recursos que estão associados à sua conta.

Tópicos

Autenticação

Você tem acesso a AWS qualquer um dos seguintes tipos de identidades:

- AWS usuário raiz da conta — Ao criar uma AWS conta pela primeira vez, você começa com uma identidade que tem acesso completo a todos os AWS serviços e recursos da conta. Essa identidade é chamada de usuário-raiz da conta da AWS . 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, siga as práticas recomendadas para o uso do usuário-raiz somente a fim de criar seu primeiro usuário do Centro de Identidade do IAM (recomendado) ou usuário do IAM (o que 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-raiz.

- Usuário do IAM — Um usuário do IAM é uma identidade em sua AWS conta que tem permissões específicas e personalizadas. Você pode usar as credenciais de usuário do IAM para entrar em AWS páginas da Web seguras, como o AWS Management Console, os fóruns de AWS discussão ou o AWS Support Center. AWS as melhores práticas recomendam que você crie um usuário do IAM Identity Center em vez de um usuário do IAM, porque há mais risco de segurança ao criar um usuário do IAM com credenciais de longo prazo.

  Se precisar criar um usuário do IAM para determinada finalidade, além das credenciais de login, você poderá gerar chaves de acesso para cada usuário do IAM. Você pode usar essas teclas ao chamar AWS serviços programaticamente, por meio de uma das várias SDKs ou usando a Interface de Linha de AWS Comando (CLI). As ferramentas do SDK e da CLI usam as chaves de acesso para cadastrar criptograficamente sua solicitação. Se você não usa AWS ferramentas, você mesmo deve assinar a solicitação. O AWS Control Tower é compatível com o Signature versão 4, um protocolo para autenticar solicitações de API de entrada. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature versão 4 na Referência AWS geral.
- Perfil do IAM: perfil do IAM é uma identidade do IAM que você pode criar em sua conta com permissões específicas. Uma função do IAM é semelhante à de um usuário do IAM, pois é uma AWS identidade e tem políticas de permissões que determinam o que a identidade pode ou não fazer AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. 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. Os perfis do IAM com credenciais temporárias são úteis nas seguintes situações:
  - Acesso de usuário federado — em vez de criar um usuário do IAM, você pode usar identidades existentes do seu diretório de AWS Directory Service usuários corporativo ou de um provedor de identidade da web. Eles 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 federados e funções no Manual do usuário do IAM.
  - AWS acesso ao serviço — Uma função de serviço é uma função do IAM que um serviço assume para realizar ações em sua conta em seu nome. Ao configurar alguns ambientes AWS 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 os AWS recursos necessários. 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 no IAM. 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 usuário do IAM.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância da Amazon e fazendo solicitações de AWS CLI AWS ou API. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância da Amazon. Para atribuir uma AWS 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 Como usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

- Usuário do Centro de Identidade do IAM A autenticação no portal de acesso do Centro de Identidade do IAM é controlada pelo diretório que você conectou ao Centro de Identidade do IAM. No entanto, a autorização para as AWS contas que estão disponíveis para os usuários finais a partir do portal do usuário é determinada por dois fatores:
  - A quem foi atribuído acesso a essas AWS contas no console do AWS IAM Identity Center. Consulte mais informações em Acesso por logon único a Contas da AWS no Guia do usuário do AWS IAM Identity Center .
  - Que nível de permissão foi concedido aos usuários finais no console do Centro de Identidade do AWS IAM para conceder acesso apropriado a essas contas da AWS . Consulte mais informações em Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center .

Controle de acesso

Para criar, atualizar, excluir ou listar recursos do 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 permissões para o AWS Control Tower:

Tópicos

- Visão geral do gerenciamento de permissões de acesso aos recursos do AWS Control Tower
- Uso de 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.

Consulte mais informações sobre como selecionar um provedor de identidades em Orientações sobre o Centro de Identidade do IAM.

Para um breve tutorial sobre como configurar seus usuários e permissões do Centro de Identidade do IAM no AWS Control Tower, assista 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 Centro de Identidade do IAM

Quando você configura inicialmente o AWS Control Tower, somente o usuário-raiz e todos os usuários do IAM com as permissões corretas podem adicionar usuários do Centro de Identidade do IAM. No entanto, depois que os usuários finais forem adicionados ao grupo AWSAccountFactory, eles poderão criar novos usuários do IAM Identity Center a partir do assistente Account Factory. Para obter mais informações, consulte Provisione e gerencie contas com o Account Factory.

Se você escolher o padrão recomendado, o AWS Control Tower configurará a zona de pouso com um diretório pré-configurado que ajuda você a gerenciar identidades de usuário e logon único, para

que seus usuários tenham acesso federado entre contas. Quando você configura a zona de pouso, 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, perfis 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-membros 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 distintos de permissões de usuário, como acesso somente leitura, acesso administrativo do AWS Control Tower e acesso do 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.

Consulte dicas sobre como planejar suas alocações de usuários, grupos e permissões em Recomendações para configurar grupos, perfis e políticas

Consulte mais informações sobre como usar esse serviço no contexto do AWS Control Tower nos tópicos a seguir no Guia do usuário do AWS IAM Identity Center .

- 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 Centro de Identidade do IAM em sua região de origem. Se você configurar a zona de pouso em outra região e acessar o console do Centro de Identidade do IAM, será necessário alterar a região para a região de origem. Não exclua a configuração do Centro de Identidade do IAM na região de origem.

O que você deve saber sobre as contas do Centro de Identidade do IAM e o AWS Control Tower

Veja a seguir alguns aspectos positivos que você deve saber ao trabalhar com contas de usuários do Centro de Identidade do IAM 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 habilitar novamente o usuário do Centro de Identidade do IAM no console do Centro de Identidade do IAM.
- Se você especificar um novo endereço de e-mail de usuário do Centro de Identidade do IAM ao atualizar o produto provisionado associado a uma conta fornecida pelo Account Factory, o AWS Control Tower criará uma conta de usuário do Centro de Identidade do IAM. A conta de usuário criada anteriormente não será removida. Se você preferir remover o endereço de e-mail anterior do usuário do Centro de Identidade do IAM do Centro de Identidade do AWS IAM, 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 Centro de Identidade do IAM para o AWS Control Tower

O AWS Control Tower oferece grupos pré-configurados para organizar os usuários que realizam tarefas específicas nas contas. Você pode adicionar usuários e atribuí-los a esses grupos diretamente no Centro de Identidade do IAM. Isso corresponde a conjuntos de permissões para usuários em grupos dentro das contas. Para obter as orientações e as melhores práticas mais

recentes sobre como configurar seus grupos, consulte as melhores práticas no Guia do usuário do IAM Identity Center.

Os grupos a seguir são criados quando você configura a zona de pouso.

AWSAccountFábrica

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 grupo AWSAccountFábrica.

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	Conjuntos de permissões	Descrição
Conta de auditoria	AWSAdministratorAccess	Os usuários dessa conta têm acesso de administrador.
Contas-membros	AWSOrganizationsFullAccess	Os usuários dessa conta têm acesso total ao Organizations.

AWSSecurityAuditPowerUsers

Conta	Conjuntos de permissões	Descrição
Conta de gerenciamento	AWSPowerUserAccess	Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configura r recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativ os.
Conta de arquivamento de logs	AWSPowerUserAccess	Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configura r recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativ os.
Conta de auditoria	AWSPowerUserAccess	Os usuários podem realizar tarefas de desenvolvimento de aplicativos e criar e configura r recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativ os.
Contas-membros	AWSPowerUserAccess	Os usuários podem realizar tarefas de desenvolvimento de

Conta	Conjuntos de permissões	Descrição
		aplicativos e criar e configura r recursos e serviços que suportem o desenvolvimento AWS consciente de aplicativ os.

AWSSecurityAuditores

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-membros	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 do AWS Control Tower

Cada AWS 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 de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e funções). Alguns serviços (como AWS Lambda) também oferecem suporte à anexação de políticas de permissões aos recursos.

> **Note**
>
> Um administrador da conta (ou administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Quando você é responsável por conceder permissões a um usuário ou perfil, deve conhecer e monitorar os usuários e perfis que exigem permissões, os recursos para os quais cada usuário e perfil exigem permissões e as ações específicas que devem ser permitidas para operar esses recursos.

Tópicos

- Recursos e operações do AWS Control Tower
- Sobre o proprietário dos recursos
- Gerenciar acesso a recursos
- Especificar elementos da política: ações, efeitos e entidades principais
- Especificar condições em uma política

Recursos e operações do AWS Control Tower

No AWS Control Tower, o recurso principal é uma zona de pouso. O AWS Control Tower também é compatível com um tipo de recurso adicional, os controles, às vezes chamados de barreiras de proteção. No entanto, para o AWS Control Tower, você pode gerenciar controles somente no contexto de uma zona de pouso existente. Os controles podem ser chamados de sub-recursos.

Os recursos e sub-recursos em AWS têm nomes de recursos da Amazon (ARNs) exclusivos associados a eles, conforme mostrado no exemplo a seguir.

O AWS Control Tower fornece um conjunto de operações de API para trabalhar com os recursos do AWS Control Tower. Consulte uma lista das operações disponíveis na Referência de API do AWS Control Tower.

Para obter mais informações sobre os AWS CloudFormation recursos no AWS Control Tower, consulte o Guia AWS CloudFormation do usuário.

Sobre o proprietário dos recursos

A AWS conta é proprietária dos recursos criados na conta, independentemente de quem criou os recursos. Especificamente, o proprietário do recurso é a AWS conta da entidade principal (ou seja, o usuário Conta da AWS raiz, um usuário do IAM Identity Center, um usuário do IAM ou uma função do IAM) que autentica a solicitação de criação do recurso. Os seguintes exemplos mostram como isso funciona:

- Se você usar as AWS credenciais de usuário raiz da sua AWS conta para configurar uma landing zone, sua AWS conta é a proprietária do recurso.
- Se você criar um usuário do IAM em sua AWS conta e conceder permissões para configurar uma landing zone para esse usuário, o usuário poderá configurar uma landing zone, desde que a conta atenda aos pré-requisitos. No entanto, sua AWS conta, à qual o usuário pertence, é proprietária do recurso landing zone.
- Se você criar uma função do IAM em sua AWS conta com permissões para configurar uma landing zone, qualquer pessoa que possa assumir a função poderá configurar uma landing zone. A sua conta da AWS à qual o perfil pertence é proprietária do recurso da zona de pouso.

Gerenciar acesso a recursos

Uma 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 aborda o uso do IAM no contexto do AWS Control Tower. Não são fornecidas informações detalhadas sobre o serviço IAM. Para obter a documentação completa do IAM, consulte O que é o IAM? no Guia do usuário do IAM. Para obter mais informações sobre a sintaxe e as descrições da política do IAM, consulte a Referência de política do AWS IAM no Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM). As políticas anexadas a um recurso são chamadas de políticas baseadas em recursos.

> **Note**
>
> O AWS Control Tower é compatível apenas com as políticas baseadas em identidade (políticas do IAM).

Tópicos

Sobre políticas baseadas em identidade (políticas do IAM)

Você pode anexar políticas a identidades do IAM. Por exemplo, você pode fazer o seguinte:

- Anexar uma política de permissões um usuário ou grupo em sua conta: para conceder a um usuário permissões para criar um recurso do AWS Control Tower, como configurar uma zona de pouso, você pode anexar uma política de permissões a um usuário ou grupo a qual o usuário pertence.
- Anexar uma política de permissões a uma função: você pode anexar uma política de permissões baseada em identidade a um perfil do IAM para conceder permissões entre contas. Por exemplo, um administrador de uma AWS 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 outro AWS serviço.
  1. O administrador da Conta A cria um perfil do IAM e anexa uma política de permissões ao perfil que concede permissões para gerenciar recursos na Conta A.
  2. O administrador da Conta A associa uma política de confiança ao perfil. A política identifica a conta B como a entidade principal que pode assumir a função.
  3. Como entidade principal, o administrador da Conta B pode dar permissão a qualquer usuário da Conta B para assumir o perfil. Ao assumir o perfil, os usuários na Conta B podem criar ou obter acesso aos recursos na Conta A.
  4. Para conceder a um AWS serviço a capacidade (permissões) de assumir a função, o principal que você especifica na política de confiança pode ser um AWS serviço.

Criar perfil e atribuir permissões

Perfis e permissões dão acesso a recursos, no AWS Control Tower e em outros serviços da AWS , 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 Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para obter mais informações sobre o uso do IAM para delegar permissões, consulte Gerenciamento de acesso no Guia do usuário do IAM.

> **Note**
>
> Ao configurar uma landing zone do 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) (console do IAM)

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Perfis e, em seguida, Criar perfil.

3. Em 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.

      O IAM inclui uma lista das políticas AWS 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 dentro de você Conta da AWS e não podem ser diferenciados por maiúsculas e minúsculas.
   >
   >   Por exemplo, não crie dois perfis denominados **`PRODROLE`** e **`prodrole`**. Quando usado em uma política ou como parte de um ARN, o nome de perfil diferencia

maiúsculas de minúsculas. No entanto, quando exibido para os clientes no console, como durante o processo de login, o nome de perfil 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 no IAM, consulte Tags para AWS Identity and Access Management recursos no Guia do usuário do IAM.
13. Reveja a função e escolha Criar função.

Para usar o editor de políticas JSON para criar uma política

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha 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 opção JSON.
5. Insira ou cole um documento de política JSON. Para obter detalhes sobre a linguagem da política do IAM, consulte a referência de política JSON do IAM.
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 de editor Visual e JSON a qualquer momento. Porém, se você fizer alterações ou escolher Próximo no editor Visual, o IAM poderá reestruturar a política a fim de otimizá-la para o editor visual. Para obter mais informações, consulte Restruturação de política no Guia do usuário do IAM.

7. (Opcional) Ao criar ou editar uma política no AWS Management Console, você pode gerar um modelo de política JSON ou YAML que pode ser usado em AWS CloudFormation modelos.

   Para fazer isso, no editor de políticas, escolha Ações e, em seguida, escolha Gerar CloudFormation modelo. Para saber mais AWS CloudFormation, consulte a referência do tipo de AWS Identity and Access Management recurso no Guia AWS CloudFormation 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 no IAM, consulte Tags para AWS Identity and Access Management recursos no Guia do usuário do IAM.
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 console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação à esquerda, escolha 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 escolha um AWS service (Serviço da AWS). Você pode usar a caixa de pesquisa na parte superior para limitar os resultados da 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 o IAM nega por padrão, a prática recomendada de segurança é que você conceda permissões somente para as ações e os recursos de que um usuário precisa. Crie uma instrução JSON para negar permissões se desejar substituir, separadamente, uma permissão que é concedida por uma outra instrução 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 editor visual de ARN ou a lista ARNs manualmente. Para obter mais informações sobre a sintaxe do ARN, consulte Amazon Resource Names (ARNs) no Guia do usuário do IAM. Para obter informações sobre o uso ARNs no `Resource` elemento de uma política, consulte Elementos de política JSON do IAM: recurso no Guia do usuário do IAM.
   - 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 de uma instrução de política JSON. 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 as condições mais 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, depois, insira um Valor. Para adicionar mais de um valor, escolha Adicionar. Você pode considerar os valores como sendo conectados por um operador lógico `OR`. 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 como sendo conectadas por um operador lógico `AND`.

Consulte mais informações sobre o elemento Condição em IAM JSON policy elements: Condition no Guia do usuário do IAM.

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 de editor Visual e JSON a qualquer momento. Porém, se você fizer alterações ou escolher Próximo no editor Visual, o IAM poderá reestruturar a política a fim de otimizá-la para o editor visual. Para obter mais informações, consulte Restruturação de política no Guia do usuário do IAM.

9. (Opcional) Ao criar ou editar uma política no AWS Management Console, você pode gerar um modelo de política JSON ou YAML que pode ser usado em AWS CloudFormation modelos.

   Para fazer isso, no editor de políticas, escolha Ações e, em seguida, escolha Gerar CloudFormation modelo. Para saber mais AWS CloudFormation, consulte a referência do tipo de AWS Identity and Access Management recurso no Guia AWS CloudFormation 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 no IAM, consulte Tags para AWS Identity and Access Management recursos no Guia do usuário do IAM.
13. Escolha Criar política para salvar sua nova política.

Como conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas 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
Identidade da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de ferramentas AWS SDKs e ferramentas.
IAM	Use credenciais temporárias para assinar solicitações	Siga as instruções em Como usar credenciais temporárias

Qual usuário precisa de acesso programático?	Para	Por
	programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	com AWS recursos no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para isso AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

Proteção contra invasores

Para obter mais informações sobre como ajudar a se proteger contra invasores ao conceder permissões a outros diretores de AWS serviço, consulte Condições opcionais para as relações de confiança de sua função. Ao adicionar determinadas condições às suas políticas, você pode ajudar a evitar um tipo específico de ataque, conhecido como ataque confused deputy, que ocorre se uma entidade coagir uma entidade com mais privilégios a realizar uma ação, como a falsificação

de identidade entre serviços. Também consulte informações gerais sobre condições de política em Especificar condições em uma política.

Consulte mais informações sobre como usar políticas baseadas em identidade com o AWS Control Tower em Uso de 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 usuário do IAM.

Políticas baseadas em recursos

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. O AWS Control Tower não é compatível com políticas baseadas em recurso.

Especificar elementos da política: ações, efeitos e entidades principais

Você pode configurar e gerenciar sua zona de pouso por meio do console do AWS Control Tower ou da landing zone APIs. Para configurar a zona de pouso, você deverá ser um usuário do IAM com permissões administrativas, conforme definido em uma política do IAM.

Estes elementos são os mais básicos que você pode identificar em uma política:

- Recurso: em uma política, você usa um Amazon Resource Name (ARN – Nome do recurso da Amazon) para identificar o recurso a que a política se aplica. Para obter mais informações, consulte Recursos e operações do AWS Control Tower.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Consulte informações sobre os tipos de ações disponíveis para serem executadas em Actions defined by 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.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. 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). O AWS Control Tower não é compatível com políticas baseadas em recurso.

Para saber mais sobre a sintaxe e as descrições da política do IAM, consulte a Referência de política do AWS IAM no Guia do usuário do IAM.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar as condições de quando uma política deverá entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Condition no Guia do usuário do IAM.

Para expressar condições, você pode usar chaves de condição predefinidas. Não existem chaves de condição específicas para o AWS Control Tower. No entanto, existem chaves AWS de condição abrangentes que você pode usar conforme apropriado. Para obter uma lista completa AWS de chaves abrangentes, consulte Chaves disponíveis para condições no Guia do usuário do IAM.

Evitar personificação entre serviços

Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. Quando um serviço chama outro, a personificação entre serviços ocorre se um serviço manipula o outro para que ele use as respectivas permissões com o objetivo de acessar os recursos do cliente de uma forma na qual ele não é permitido. 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 o uso das condições `aws:SourceArn` e `aws:SourceAccount` em suas políticas para limitar as permissões que o AWS Control Tower concede a outro serviço para acessar seus recursos.

- Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços.
- Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.
- Se o valor de `aws:SourceArn` 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 utilizar ambas as condições e o valor de `aws:SourceArn` contiver o ID da conta, o valor de `aws:SourceAccount` e a conta no valor de `aws:SourceArn` deverão utilizar o mesmo ID de conta quando usado na mesma instrução de política.

Para ter mais informações e exemplos, consulte https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

Uso de 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 a identidades do IAM (ou seja, usuários, grupos e perfis) e, assim, conceder permissões para realizar operações em recursos do AWS Control Tower.

> **Important**
>
> Recomendamos analisar primeiro os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos recursos do AWS Control Tower. Para obter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos recursos do AWS Control Tower.

Permissões obrigatórias para usar o console do AWS Control Tower

O AWS Control Tower cria três perfis automaticamente quando você configura uma zona de pouso. Todos os três perfis são necessários para permitir o acesso ao console. O AWS Control Tower divide as permissões em três perfis como uma prática recomendada para restringir o acesso ao mínimo de conjuntos de ações e recursos.

Três perfis necessários

- AWS ControlTowerAdmin papel
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Recomendamos que você restrinja o acesso às políticas de confiança de perfil a esses perfis. Consulte mais informações em Optional conditions for your role trust relationships.

AWS ControlTowerAdmin papel

Esse perfil concede ao AWS Control Tower o acesso à infraestrutura essencial para manter a zona de pouso. O perfil `AWS ControlTowerAdmin` exige uma política gerenciada anexada e uma política de confiança de perfil para o perfil do IAM. Uma política de confiança de perfil é uma política baseada no recurso que especifica quais entidades principais podem assumir o perfil.

Aqui está um exemplo de política de confiança de perfil:

```
{
  "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
```

Esse perfil 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`.

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.

Consulte mais informações em `AWSControlTowerServiceRolePolicy` no Guia de referência de políticas gerenciadas pela AWS.

Política de confiança de perfil:

```
{
    "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. CloudTrail assume 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 o perfil `AWSControlTowerBlueprintAccess` na conta designada do hub de esquemas designada, dentro da mesma organização.

Nome da função

O tipo de função deve ser `AWSControlTowerBlueprintAccess`.

Política de confiança de perfil

O perfil deve ser configurado para confiar nestas entidades principais:

- A entidade principal que usa o AWS Control Tower na conta de gerenciamento.
- O perfil `AWSControlTowerAdmin` na conta de gerenciamento.

O exemplo a seguir mostra uma política de confiança de privilégio mínimo. Ao criar sua própria política, substitua o termo *YourManagementAccountId* pelo ID da conta real da conta de gerenciamento do AWS Control Tower e substitua o termo *YourControlTowerUserRole* pelo identificador do perfil do IAM da 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 do perfil

Você deve anexar a política gerenciada AWSServiceCatalogAdminFullAccessà função.

AWSServiceRoleForAWSControlTorre

Esse perfil fornece ao AWS Control Tower acesso à conta de arquivamento de logs, à conta de auditoria e às contas-membros para operações essenciais de manutenção da zona de pouso, como notificar você sobre recursos com desvio.

O perfil `AWSServiceRoleForAWSControlTower` exige uma política gerenciada anexada e uma política de confiança de perfil para o perfil do IAM.

Política gerenciada para esse perfil: `AWSControlTowerAccountServiceRolePolicy`

Política de confiança de perfil:

```
{
    "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 o AWS Control Tower implementar o encaminhamento de descobertas do AWS Security Hub 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. Faz parte do processo de detecção de desvios do AWS Security Hub 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 membro, e essas regras devem especificar uma exata EventPattern.

Além disso, uma regra pode operar somente em regras gerenciadas por nossa entidade principal do serviço.

Entidade principal do serviço: `controltower.amazonaws.com`

Para obter mais informações, consulte `AWSControlTowerAccountServiceRolePolicy`o Guia de referência de políticas AWS gerenciadas.

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
AWS ControlTowerServiceRolePolicy: atualizar para uma política existente	O AWS Control Tower adicionou novas permissões que permitem que o AWS Control Tower faça chamadas para o AWS CloudFormation serviço APIs `ActivateType DeactivateType SetTypeConfiguration` , e assim por dianteAWS::ControlTower types. Essa mudança permite que os clientes provisionem controles proativos sem a implantação de tipos de AWS CloudFormation Hook privados.	10 de dezembro de 2024

Alteração	Descrição	Data
AWSControlTowerAccountServiceRolePolicy: uma nova política	O AWS Control Tower adicionou um novo perfil vinculado ao serviço que permite que o 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. Essa mudança é necessária para que os clientes possam visualizar recursos com desvio no console, quando esses recursos estão relacionados aos controles do Security Hub que fazem parte do padrão gerenciado pelo serviço do Security Hub: AWS Control Tower.	22 de maio de 2023

Alteração	Descrição	Data
AWS ControlTowerServiceRolePolicy: atualizar para uma política existente	A AWS Control Tower adicionou novas permissões que permitem que a AWS Control Tower faça chamadas para `EnableRegion` , `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). Essa mudança é necessária para que os clientes tenham a opção de expandir a governança de região do AWS Control Tower para as regiões opcionais.	6 de abril de 2023

Alteração	Descrição	Data
AWS ControlTowerServiceRolePolicy: atualizar para uma política existente	O AWS Control Tower adicionou novas permissões que autorizam o AWS Control Tower a assumir o perfil `AWSControlTowerBlueprintAccess` na conta de esquema (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 o perfil `AWSControlTowerBlueprintAccess` para realizar três tarefas: criar um portfólio do Service Catalog, adicionar o produto do esquema solicitado e compartilhar o portfólio com uma conta-membro solicitada no momento do provisionamento da conta. Essa alteração é necessária para que os clientes possam provisionar contas personalizadas por meio do Account Factory do AWS Control Tower.	28 de outubro de 2022

Alteração	Descrição	Data
AWS ControlTowerServiceRolePolicy: atualizar 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. 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: atualizar para uma política existente	O AWS Control Tower adicionou novas permissões que autorizam os clientes a usar a criptografia de chaves do KMS. O recurso KMS permite que os clientes forneçam sua própria chave KMS para criptografar seus registros. CloudTrail Os clientes também podem alterar a chave do KMS durante a atualização ou o reparo da zona de pouso. 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
AWS Control Tower começou a monitorar alterações	O AWS Control Tower começou a monitorar as mudanças em suas políticas AWS gerenciadas.	27 de maio de 2021

Segurança no 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 Serviços da AWS no escopo por programa de conformidade.
- 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.

Esta 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 aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do AWS Control Tower.

Proteção de dados no AWS Control Tower

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no 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 o 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 a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

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 uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de 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 módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags 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 AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em 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 fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

> **Note**
>
> O registro de atividades do usuário com AWS CloudTrail é processado automaticamente no AWS Control Tower quando você configura sua landing zone.

Consulte mais informações sobre proteção de dados na publicação do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS . O AWS Control Tower oferece as seguintes opções que você pode usar para ajudar a proteger o conteúdo que existe na zona de pouso:

Tópicos

Criptografia em repouso

O AWS Control Tower usa buckets do S3 e bancos de dados do Amazon DynamoDB que são criptografados em repouso usando chaves gerenciadas pelo Amazon S3 (SSE-S3) para oferecer suporte à zona de pouso. Essa criptografia é configurada por padrão quando você configura a zona de pouso. Opcionalmente, você pode configurar a zona de pouso para criptografar recursos com chaves de criptografia do KMS. Também é possível estabelecer a criptografia em repouso para os serviços que você usa na zona de pouso compatíveis com ela. Consulte mais informações no capítulo sobre segurança da documentação online do serviço.

Criptografia em trânsito

O AWS Control Tower usa o Transport Layer Security (TLS) e a criptografia do lado do cliente para a criptografia em trânsito em suporte à zona de pouso. Além disso, o acesso ao AWS Control Tower requer o uso do console, que só pode ser acessado por meio de um endpoint HTTPS. Essa criptografia é configurada por padrão quando você configura a zona de pouso.

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 os administradores da nuvem central os e usuários finais tenham as permissões do IAM corretas ou, no caso de usuários do Centro de Identidade do IAM, que eles estejam nos grupos corretos.

- Para obter mais informações sobre as políticas e perfis para entidades do IAM, consulte o Guia do usuário do IAM.

- Consulte mais informações sobre os grupos do Centro de Identidade do IAM que são criados quando você configura a zona de pouso em Grupos do Centro de Identidade do IAM para o AWS Control Tower.

Validação de conformidade do AWS Control Tower

O AWS Control Tower é um serviço bem arquitetado que pode ajudar a sua organização a atender às necessidades de conformidade com proteções e práticas recomendadas. Além disso, auditores independentes avaliam a segurança e a conformidade de uma série de serviços que você pode usar na zona de pouso como parte de vários programas de conformidade da AWS . Isso inclui SOC, PCI, FedRAMP, HIPAA 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 dos 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 segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos compatíveis com a HIPAA.
- 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 no 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 center tradicionais.

Para obter uma lista de Regiões da AWS onde o AWS Control Tower está disponível, consulteComo AWS as regiões funcionam com o 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 no AWS Control Tower

O AWS Control Tower é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa chamadas de API 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 ter compatibilidade com conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece compatibilidade com esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

É possível configurar grupos de segurança para fornecer segurança adicional de infraestrutura de rede para suas workloads da zona de pouso do AWS Control Tower. Para obter mais informações,

consulte Passo a passo: configure grupos de segurança no AWS Control Tower com AWS Firewall Manager.

Registro em log e monitoramento no 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 em log e o monitoramento são conceitos intimamente relacionados e são uma parte importante da natureza bem arquitetada do AWS Control Tower.

Quando você configura a zona de pouso, uma das contas compartilhadas criadas é a conta de arquivamento de logs. Ele se dedica a coletar todos os logs centralmente, incluindo logs de todas as suas contas compartilhadas e de contas-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 configuração da AWS em seus logs para ser mais fácil realizar a depuração de uma falha de vários pontos, caso ocorra. O AWS fornece várias ferramentas para monitorar seus recursos e atividades na zona de pouso.

Por exemplo, o status dos controles é monitorado constantemente. Você pode ver seu status rapidamente no console do AWS Control Tower ou programaticamente por meio do AWS Control Tower. APIs A integridade e o status das contas que você provisionou no Account Factory também são monitorados constantemente.

Visualizar ações registradas em log na página Atividades

No console do AWS Control Tower, a página Atividades fornece uma visão geral das ações da conta de gerenciamento do AWS Control Tower. Para acessar a página Atividades do AWS Control Tower, selecione Atividades na 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).

É possível visualizar ações e eventos de contas-membros nos arquivos de arquivamento de logs.

As seções a seguir descrevem o monitoramento e o registro em log no AWS Control Tower com mais detalhes:

Tópicos

Sobre o registro em log 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 em log, incluindo aquelas das contas de gerenciamento do AWS Control Tower e das contas-membros da organização. As ações e os eventos da conta de gerenciamento podem ser visualizados na página Atividades no console. É possível visualizar ações e eventos de contas-membros nos arquivos de arquivamento de logs.

Trilhas no nível da organização

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 em log todos os eventos para a conta de gerenciamento e todas as contas-membros da organização. Esse recurso depende de acesso confiável para dar à conta de gerenciamento permissões para criar uma trilha em cada conta-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 da zona de pouso, o AWS Control Tower criou uma trilha de conta-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 zona de pouso, o AWS Control Tower exclui as trilhas no nível da conta (que o AWS Control Tower criou) nas suas contas inscritas em seu nome. Seus arquivos de log existentes no nível da conta são preservados em seu bucket do 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 condição `aws:SourceOrgID` deve ser atendida para qualquer permissão de gravação.

É possível usar a chave de condição `aws:SourceOrgID` e definir o valor do ID da organização no elemento de condição da 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 das workloads 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. Você pode 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 EC2 instâncias da Amazon 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 de EC2 instâncias da Amazon 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 visualizar e consultar a CloudTrail atividade em uma conta por meio do CloudWatch Logs e do CloudWatch Logs Insights. Essa atividade inclui eventos de ciclo de vida do AWS Control Tower. CloudWatch Os recursos dos registros permitem que você realize consultas mais granulares e precisas do que você normalmente seria capaz de fazer usando. CloudTrail

Para obter 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 não configurar uma trilha, você ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history. 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 da zona de pouso, o AWS Control Tower criou uma trilha de conta-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, quando uma trilha é criada no console, a mesma 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:

- Visão Geral para Criar uma Trilha
- Prepare for creating a trail
- 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:

Público APIs

- Para obter uma lista completa do público da AWS Control Tower APIs e detalhes sobre cada um, consulte The AWS Control Tower API Reference. As chamadas para esses públicos APIs são registradas por AWS CloudTrail.

Outros 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 o seguinte:

- 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 uma função 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 Elemento userIdentity do CloudTrail .

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 (IC), 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 zona de pouso for 3.0 ou posterior: o AWS Control Tower limita a gravação de recursos globais, como políticas gerenciadas pelo cliente, perfis, grupos e usuários do IAM somente

à sua região de origem. As cópias das alterações de recursos globais 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 tem 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 informações desta seção podem não se aplicar à sua zona de pouso.

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 perfis do IAM, são registrados uma vez por região. Por exemplo, se você criar uma nova função do IAM em uma conta cadastrada que está operando em cinco regiões, AWS Config gera cinco CIs, uma 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 zona hospedada do Route 53 em uma conta inscrita, o AWS Config gerará uma IC, independentemente de quantas regiões estejam selecionadas para essa conta. Consulte uma lista que ajuda você a distinguir esses tipos de recursos em O 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 de API Descrever de outro recurso, eles 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 EC2 instância da Amazon e a API exigir que você crie uma interface de rede, AWS Config considere que a EC2 instância da Amazon 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 EC2 instância da Amazon associada que faz parte do grupo de segurança.

Consulte mais informações sobre relações diretas e indiretas em What is a direct and an indirect relationship with respect to a resource?

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 CIs 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 `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 o painel de conformidade do Config Resource e a 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 grandes números, esse fluxo de trabalho pode gerar um grande número de CIs. Se você executar esses processos em uma conta que não seja de produção, considere cancelar o registro 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.

Consulte mais informações em Unmanage an enrolled account. Para saber como desativar o AWS Config gravador, consulte Gerenciando o gravador de configuração.

O mesmo recurso é registrado várias vezes

Verifique se é um recurso 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. Estes são 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 em log 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 uma landing zone, uma linha de base ou um controle, relacionados a uma unidade organizacional (OU) ou conta.

Características dos eventos de 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 UO, o AWS Control Tower inicia 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 de ciclo de vida inclui um carimbo de data/hora registrado no log que mostra quando a ação do AWS Control Tower foi iniciada, e outro carimbo de data/hora que mostra quando o evento de ciclo de vida foi concluído, indicando o êxito ou a falha.

Visualizar eventos de ciclo de vida no Control Tower

Você pode visualizar eventos de 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.

Consulte mais informações sobre como integrar eventos de ciclo de vida do AWS Control Tower em seus fluxos de trabalho nesta publicação do blog Using lifecycle events to track AWS Control Tower actions and trigger automated workflows.

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. Caso haja um erro durante o processo, ele costuma ocorrer depois que a conta é criada, mas antes de estar 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 de ciclo de vida `UpdateManagedAccount` em vez do evento de ciclo de vida `CreateManagedAccount` no final da solicitação de nova tentativa. Talvez você veja outro evento `CreateManagedAccount` por causa

do erro. No entanto, o evento de ciclo de vida do `UpdateManagedAccount` 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 log registra se o AWS Control Tower concluiu todas as ações para criar e provisionar uma nova conta usando o Account Factory com êxito.
- `UpdateManagedAccount`: o log registra se o AWS Control Tower concluiu todas as ações para atualizar um produto provisionado que está associado a uma conta que você tinha criado anteriormente utilizando o Account Factory com êxito.
- `EnableGuardrail`: o log registra se todas as ações do AWS Control Tower foram concluídas com êxito para habilitar um controle em uma UO criada pelo AWS Control Tower.
- `DisableGuardrail`: o log registra se todas as ações do AWS Control Tower foram concluídas com êxito para desabilitar um controle em uma UO criada pelo AWS Control Tower.
- `SetupLandingZone`: o log registra se o AWS Control Tower concluiu todas as ações para configurar uma zona de pouso com êxito.

- `UpdateLandingZone`: o log registra se o AWS Control Tower concluiu todas as ações para atualizar a zona de pouso existente com êxito.
- `RegisterOrganizationalUnit`: o log registra se o AWS Control Tower concluiu todas as ações para habilitar os recursos de governança dele em uma UO com êxito.
- `DeregisterOrganizationalUnit`: o log registra se o AWS Control Tower concluiu todas as ações para desabilitar os recursos de governança dele em uma UO com êxito.
- `PrecheckOrganizationalUnit`: o log registra se o AWS Control Tower detectou algum recurso que impediria a conclusão da operação de Estender governança com êxito.
- `EnableBaseline`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para habilitar uma nova linha de base em uma conta de membro alvo em uma OU. A operação de ativação pode ser iniciada usando a `EnableBaseline` API ou o console.
- `ResetEnabledBaseline`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para redefinir uma linha de base existente habilitada em uma conta de membro alvo em uma OU. A operação de redefinição pode ser iniciada usando a `ResetEnabledBaseline` API ou o console.
- `UpdateEnabledBaseline`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para atualizar uma linha de base habilitada existente em uma conta de membro alvo em uma OU. A operação de atualização pode ser iniciada usando a `UpdateEnabledBaseline` API ou o console.
- `DisableBaseline`: o registro registra se o AWS Control Tower concluiu com sucesso todas as ações para desativar uma linha de base habilitada existente em uma conta de membro alvo em uma OU. A operação de desativação pode ser iniciada usando a `DisableBaseline` API ou o console.

As seções a seguir fornecem uma lista de eventos de ciclo de vida do AWS Control Tower, com exemplos dos detalhes registrados em log para cada tipo de evento de ciclo de vida.

`CreateManagedAccount`

Este evento de ciclo de vida registra se o AWS Control Tower criou e provisionou uma nova conta usando o Account Factory com êxito. 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

Este evento de ciclo de vida registra se o AWS Control Tower teve êxito ao atualizar o produto provisionado associado a uma conta que foi criada anteriormente usando o Account Factory. 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":"XXXXXXXXXXXX"
                    },
                "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

Este evento de ciclo de vida registra se o AWS Control Tower teve êxito ao habilitar um controle em uma UO que está sendo gerenciada pelo AWS Control Tower. Esse evento corresponde ao evento AWS Control Tower `EnableGuardrail` CloudTrail . O log de eventos de ciclo de vida inclui o `guardrailId` e `guardrailBehavior` do controle, e o `organizationalUnitName` e `organizationalUnitId` da UO em que o controle está habilitado.

```
{
    "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

Este evento de ciclo de vida registra se o AWS Control Tower teve êxito ao desabilitar um controle em uma UO que está sendo gerenciada pelo AWS Control Tower. Esse evento corresponde ao evento AWS Control Tower `DisableGuardrail` CloudTrail . O log de eventos de ciclo de vida inclui o `guardrailId` e `guardrailBehavior` do controle, e o `organizationalUnitName` e `organizationalUnitId` da UO em que o controle está desabilitado.

```
{
```

```
    "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

Este evento de ciclo de vida registra se o AWS Control Tower configurou uma zona de pouso com êxito. Esse evento corresponde ao evento AWS Control Tower `SetupLandingZone` CloudTrail . O log de eventos de ciclo de vida inclui o `rootOrganizationalId`, que é o ID da organização que o AWS Control Tower cria da conta de gerenciamento. A entrada de registro também inclui o `organizationalUnitName` e `organizationalUnitId` para cada uma das OUs, e o `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 a zona de pouso existente com êxito. Esse evento corresponde ao evento AWS Control Tower `UpdateLandingZone`

CloudTrail . O log de eventos de ciclo de vida inclui o `rootOrganizationalId`, que é o ID da organização (atualizada) administrada pelo AWS Control Tower. A entrada de registro também inclui o `organizationalUnitName` e `organizationalUnitId` para cada uma das OUs, e o `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 os recursos de governança com êxito em uma UO. Esse evento corresponde ao evento AWS Control Tower `RegisterOrganizationalUnit` CloudTrail . O log de eventos de ciclo de vida inclui o `organizationalUnitName` e `organizationalUnitId` da UO 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 desabilitou os recursos de governança com êxito em uma UO. Esse evento corresponde ao evento AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail . O log de eventos de ciclo de vida inclui o `organizationalUnitName` e `organizationalUnitId` da UO em que o AWS Control Tower desabilitou os 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 de ciclo de vida registra se o AWS Control Tower realizou as pré-verificações em uma UO com êxito. Esse evento corresponde ao evento AWS Control Tower `PrecheckOrganizationalUnit` CloudTrail . O log de eventos de ciclo de vida contém um campo para os valores `Id`,`Name` e `failedPrechecks` para cada recurso no qual o AWS Control Tower realizou pré-verificações durante o processo de registro da UO.

O log de eventos também contém informações sobre as contas aninhadas nas quais as pré-verificações foram realizadas, incluindo os campos `accountName`, `accountId` e `failedPrechecks`.

Se o valor `failedPrechecks` estiver vazio, isso indicará que todas as pré-verificações desse recurso foram aprovadas com êxito.

- Esse evento será emitido somente se houver uma falha na pré-verificação.
- Esse evento não será emitido se você estiver registrando uma UO 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"
}
```

EnableBaseline

Esse evento de ciclo de vida registra se o AWS Control Tower habilitou com sucesso uma linha de base em uma conta de membro alvo em uma OU. Esse evento corresponde à AWS Control Tower `RegisterOrganizationalUnit` ou `EnableBaseline` CloudTrail aos eventos. O registro de eventos do ciclo de vida inclui a linha de base que foi ativada e sua versão, aquela `targetIdentifier` na qual a linha de base foi ativada, a linha `parentIdentifier` de base ativada na OU principal e a `statusSummary` exibição do status BEM-SUCEDIDO ou FALHA, junto com os parâmetros adicionais e o registro de data e hora da operação.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T17:14:57Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "366911a2-4fa6-4e4a-ac2b-280f627e0027",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "enableBaselineStatus": {
```

```
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "37f5eb68-e5b9-4c70-ae76-4ca15f6b16de",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX"                          }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T17:07:09+0000",
            "completedTimestamp": "2025-02-10T17:14:57+0000"
        }
    },
    "eventCategory": "Management"
}
```


ResetEnabledBaseline

Esse evento de ciclo de vida registra se o AWS Control Tower redefiniu com sucesso a linha de base habilitada existente em uma conta de membro alvo em uma OU. Esse evento corresponde à AWS Control Tower `RegisterOrganizationalUnit` ou `ResetEnabledBaseline` CloudTrail aos eventos. O registro de eventos do ciclo de vida inclui a linha de base que foi ativada e sua versão, aquela `targetIdentifier` na qual a linha de base foi ativada, a linha `parentIdentifier` de base ativada na OU principal e a `statusSummary` exibição do status BEM-SUCEDIDO ou FALHA, junto com os parâmetros adicionais e o registro de data e hora da operação.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T21:17:55Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "ResetEnabledBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "c01a32e1-13ab-4b46-8f1b-00699ef6f989",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "resetEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "3e364c89-89fa-42b8-9776-9f7cc47ba1fa",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-02-10T21:14:24Z",
            "completedTimestamp": "2025-02-10T21:17:54+0000"
        }
    },
    "eventCategory": "Management"
}
```

UpdateEnabledBaseline

Esse evento de ciclo de vida registra se o AWS Control Tower atualizou com sucesso a linha de base existente habilitada em uma conta de membro alvo em uma OU. Esse evento corresponde à AWS Control Tower `RegisterOrganizationalUnit` ou `UpdateEnabledBaseline` CloudTrail aos eventos. O registro de eventos do ciclo de vida inclui a linha de base que foi ativada e sua versão, aquela `targetIdentifier` na qual a linha de base foi ativada, a linha `parentIdentifier` de base ativada na OU principal e a `statusSummary` exibição do status BEM-SUCEDIDO ou FALHA, junto com os parâmetros adicionais e o registro de data e hora da operação.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T19:45:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "514f2aff-1a99-4912-bda1-0d4d6662c96e",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "updateEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
```

```
                    "lastOperationIdentifier": "ba3de28f-83fb-4c9a-8a8c-a4e15fac2c41",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXX"                            }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T19:39:35+0000",
            "completedTimestamp": "2025-02-10T19:45:28+0000"
        }
    },
    "eventCategory": "Management"
}
```

DisableBaseline

Esse evento de ciclo de vida registra se o AWS Control Tower desativou com sucesso a linha de base habilitada existente em uma conta de membro alvo em uma OU. Esse evento corresponde ao evento AWS Control Tower `DisableBaseline` CloudTrail . O registro de eventos do ciclo de vida inclui a linha de base que foi ativada e sua versão, aquela `targetIdentifier` na qual a linha de base foi ativada, a linha `parentIdentifier` de base ativada na OU principal e a `statusSummary` exibição do status BEM-SUCEDIDO ou FALHA, junto com os parâmetros adicionais e o registro de data e hora da operação.

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-03-14T00:50:58Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "704794c4-a32e-4960-8386-c7efaa5a22a1",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "disableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "baselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-03-14T00:49:13Z",
            "completedTimestamp": "2025-03-14T00:50:58+0000"
```

```
        }
    },
    "eventCategory": "Management"
}
```

Usando notificações AWS de usuário com AWS Control Tower

Você pode usar as Notificações de Usuários da AWS para configurar canais de entrega para receber notificações sobre eventos do AWS Control Tower . 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 bate-papo do Amazon Q Developer em aplicativos de bate-papo ou notificações push do aplicativo móvel do AWS console. 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 ficam 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 simples.
- 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
        }
    }
}
```

AWS Backup e AWS Control Tower

AWS Backup é um serviço que permite criar planos para fazer backup automático de seus AWS recursos. Para configurar backups para seus recursos do AWS Control Tower, você deve seguir quatro etapas principais:

1. Habilite AWS Backup para sua landing zone. Você pode fazer isso na página de configurações da zona de pouso no console do AWS Control Tower. Quando você ativa AWS Backup, os recursos são criados em várias contas. Para obter mais informações, consulte Recursos criados para AWS Backup.
2. Opte por fazer backups para o AWS Control Tower no AWS Backup console. Para obter mais informações, consulte Como trabalhar com serviços compatíveis no Guia do AWS Backup desenvolvedor.
3. Ative AWS Backup a pessoa OUs que você deseja incluir. Você pode realizar essa tarefa na página de detalhes da OU no console, depois de habilitar AWS Backup no nível da landing zone. Quando você ativa AWS Backup em uma OU, as contas nessa OU recebem AWS Backup cofres locais.
4. Marque os recursos selecionados para incluir nos backups. A tag indica a frequência dos backups desse recurso. Seu plano de backup segue o cronograma especificado pelas tags de recursos em cada recurso.

Para obter mais informações, consulte o Guia do AWS Backup desenvolvedor. Não há nenhum custo quando você configura o AWS Backup com o AWS Control Tower. Você incorrerá em custos de AWS Backup. Para obter mais informações sobre preços, consulte Preços do AWS Backup.

Para obter mais detalhes sobre os AWS Backup recursos que o AWS Control Tower cria na sua zona de pouso da AWS Control Tower, consulte Recursos criados para AWS Backup

> **Note**
>
> O AWS Control Tower não oferece suporte à configuração de planos de backup para recursos da AWS Control Tower diretamente por meio do AWS Backup serviço, sem também habilitá-lo no serviço AWS Control Tower.

Pré-requisitos

Antes de poder configurar AWS Backup seus recursos do AWS Control Tower, você deve ter uma AWS Organizations organização existente. Se você já configurou sua landing zone do AWS Control Tower, ela serve como sua organização atual.

Você deve alocar ou criar duas outras AWS contas que não estejam inscritas no AWS Control Tower. Essas contas se tornam a conta de backup central e a conta do administrador de backup. Nomeie essas contas com esses nomes.

Além disso, você deve selecionar ou criar uma chave multirregional AWS Key Management Service (KMS), especificamente para Backup AWS .

Definindo seus pré-requisitos

- A conta de backup central — A conta de backup central armazena seu cofre de backup do AWS Control Tower e seus backups. Esse cofre é criado em tudo o Regiões da AWS que o AWS Control Tower governa, dentro dessa conta. Cópias entre contas são armazenadas nessa conta, caso uma conta seja comprometida e exija restauração de dados.
- A conta do administrador de backup — A conta do administrador de backup é a conta do administrador delegado para o AWS Backup serviço no AWS Control Tower. Ele armazena os planos de relatório do Backup Audit Manager (BAM). Essa conta agrega todos os dados de monitoramento de backup, como trabalhos de restauração e trabalhos de cópia. Os dados são armazenados em um bucket do Amazon S3. Para obter mais informações, consulte Criação de planos de relatório usando o AWS Backup console no Guia do AWS Backup desenvolvedor.
- Requisito de política para a chave multirregional AWS KMS

  Sua AWS KMS chave exige uma política de chaves. Considere uma política de chaves semelhante a essa, que restringe o acesso aos principais (usuários e funções) que têm permissões raiz do IAM associadas à conta de gerenciamento da sua organização:

```
{
    "Version": "2012-10-17",
    "Id": "KMS key policy",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::MANAGEMENT-ACCOUNT-ID:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the KMS key for organization",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:Encrypt",
                "kms:ReEncrypt*",
                "kms:GetKeyPolicy",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "ORGANIZATION-ID"
                }
            }
        }
    ]
}
```

> **Note**
>
> Sua AWS KMS chave multirregional deve ser replicada para cada coisa Região da AWS que você planeja governar com o AWS Control Tower.

Ativar backups

Você pode habilitar backups para recursos em suas contas que estão inscritas no AWS Control Tower, durante a configuração da zona de pouso ou ao atualizar sua zona de pouso.

ComoPré-requisitos, você deve fornecer os seguintes itens

- E Conta da AWS para servir como conta de AWS Backup administrador
- E Conta da AWS para servir como conta de Backup AWS Backup Central
- Uma AWS KMS chave multirregional que você gerencia, para backups entre contas

Como habilitar backups

O processo de capacitação tem duas partes principais: primeiro, habilite backups para sua landing zone; depois, habilite backups para cada OU registrada que exija backups.

Primeira parte: configure backups para sua landing zone

Console: você pode configurar backups para sua zona de pouso no console do AWS Control Tower, na página de configurações da zona de pouso. Você verá essa opção durante a operação inicial de configuração da zona de pouso e poderá revisitá-la posteriormente com uma atualização da zona de pouso.

API: você pode habilitar backups com a AWS Control Tower APIs, chamando a `UpdateLandingZone`API, se você já tiver uma landing zone da AWS Control Tower, ou a `CreateLandingZone`API se estiver configurando a AWS Control Tower pela primeira vez. (Dica: depois disso, chame a `EnableBaseline`API para estabelecer backups para cada UO que você precisar.)

Fora do console do AWS Control Tower

Parte da habilitação de backups para sua landing zone inclui sair do console do AWS Control Tower. Você deve navegar até o AWS Backup console para revisar seus recursos.

Para revisar seus tipos de recursos aceitos ou optar por tipos de recursos adicionais

1. Abra o AWS Backup console emhttps://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Configurações.
3. Na página Optar pela adoção do serviço, escolha Configurar recursos.
4. Use as chaves seletoras para ativar ou desativar os serviços com os quais você deseja incluir. AWS BackupCertifique-se de que os recursos dos quais você deseja fazer backup estejam selecionados, como RDS, EC2 DDB e assim por diante, independentemente de fazerem parte do seu ambiente do AWS Control Tower ou não.

Para obter mais detalhes, consulte Aceitar o gerenciamento de serviços com AWS Backup.

> **Considerações sobre novos tipos de recursos**
>
> Antes de AWS Backup confiar no gerenciamento da proteção de dados dos recursos de qualquer AWS serviço, você deve executar o procedimento anterior e optar AWS Backup por esse serviço. Além disso, à medida que o AWS Backup serviço adiciona suporte para serviços adicionais e seus tipos de recursos no futuro, você deve repetir esse procedimento e optar por cada tipo de recurso adicional AWS Backup antes de poder fazer backup desse tipo de recurso no AWS Control Tower. Marcar um tipo de recurso não suportado pode fazer com que seu backup falhe.

Quando você ativa backups para sua landing zone, o AWS Control Tower estabelece as duas contas que você forneceu como a conta de Backup Central e a conta do Administrador de Backup, respectivamente. O AWS Control Tower cria recursos nessas contas e em outras contas.

> **Important**
>
> Para habilitar backups para as contas do AWS Control Tower Audit e Log Archive, você deve configurar backups para a OU de segurança, chamando a `EnableBaseline` API. Recomendamos que você o faça.

O banco recomendado de planos e retenção é o seguinte:

- Backups de hora em hora = retenção de 2 semanas no cofre local, sem cópia no cofre de backup central
- Backups diários = retenção de 2 semanas no cofre local, retenção de 1 mês no cofre central de backup
- Backups semanais = retenção de 1 mês no cofre local, retenção de 3 meses no cofre central
- Backups mensais = retenção de 3 meses no cofre local, retenção de 3 meses no cofre de backup central

Para obter informações sobre como criar seus planos de backup, consulte Criação de planos de relatório usando o AWS Backup console.

Próxima parte: Habilitar backups em OUs

Depois de habilitar AWS Backup nas configurações da landing zone, você deve executar a etapa adicional para habilitar o backup no local específico OUs do qual deseja fazer backup. Se você habilitou AWS Backup sua landing zone, você verá uma seção na página de detalhes da OU no console, que permite escolher Habilitar backup para a OU. Se o backup não estiver habilitado no nível da landing zone, você não verá essa seção na página de detalhes da OU.

Para `BackupBaseline` habilitá-los em uma OU, essa OU já deve ter o `AWSControlTowerBaseline` ativado. As contas inscritas em cada OU têm o `AWSControlTowerBaseline` habilitado.

Nas contas selecionadas e OUs, o AWS Control Tower configura recursos adicionais

- Um cofre de Backup local

  O AWS Control Tower cria um cofre de backup local em suas contas, com quatro tipos possíveis de planos de backup anexados ao cofre. Os planos de backup criados por meio do AWS Control Tower são marcados com um prefixo.

  ```
  BackupPlanTags:
          aws-control-tower: 'managed-by-control-tower'
  ```

- Quatro tipos de planos de backup: por hora, diariamente, semanalmente e mensalmente.

  Cada plano está associado a uma atribuição de recursos com base em tags. Por exemplo, qualquer recurso marcado com aws-control-tower-backuphourly : true é protegido por um plano de backup por hora.

- Uma função de backup local em suas contas

  O AWS Control Tower cria uma função do IAM, que é usada para backups. A função requer quatro permissões específicas.

  ```
  "backup:UpdateGlobalSettings","organizations:RegisterDelegatedAdministrator","organizations:E
  ```

  A função tem uma relação de confiança com o responsável pelo serviço. AWS Backup A função é nomeada `aws-controltower-backup-role` e tem as seguintes permissões gerenciadas anexadas a ela:

  - `AWSBackupServiceRolePolicyForBackup`

- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore

Marcar recursos para backup

Parte do processo de configuração de backups no AWS Control Tower é marcar os recursos que você deseja incluir no seu plano de backup. As tags especificam a frequência dos backups. Essas são as tags possíveis.

- `aws-control-tower-backuphourly : true`
- `aws-control-tower-backupdaily: true`
- `aws-control-tower-backupweekly: true`
- `aws-control-tower-backupmonthly: true`

Considerações

- Quando AWS Backup estiver ativo em uma OU, você verá um valor de Enabled no campo Status na página de detalhes da OU no console do AWS Control Tower. Alguns outros valores possíveis do campo Status incluem Não ativado, Em andamento e Falha. Se você ver um status de Falha, escolha Registrar OU novamente para reaplicar sua AWS Backup configuração à OU.
- Se você tiver AWS Backup habilitado em uma OU, novas contas provisionadas por meio do Account Factory de acordo com as quais a OU incluirá. AWS Backup

Desativar os backups

Você pode desativar os backups de seus recursos em contas que estão inscritas no AWS Control Tower, durante a configuração da zona de pouso ou ao atualizar sua zona de pouso.

Duas etapas principais são necessárias para desativar os backups: primeiro, desative a AWS Backup linha de base em cada OU que tenha backups ativados e, em seguida, desative os backups da sua landing zone.

Primeira etapa: ativar os backups OUs

Se AWS Backup estiver ativado, você deve desativar a AWS Backup linha de base de tudo OUs antes de poder AWS Backup desligar sua landing zone.

Para desativar a AWS Backup linha de base em uma OU, você pode chamar a `DisableBaseline` API. Os aninhados OUs herdam esse status, de forma que a linha de base do AWS Backup também seja desativada para eles.

Exemplo de comando:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

Quando você desativa a AWS Backup linha de base, o AWS Control Tower limpa os seguintes recursos:

- Todos os conjuntos de pilhas relacionados a AWS Backup
- Todos os controles relacionados a AWS Backup

> **Note**
>
> O cofre local é mantido mesmo que os conjuntos de pilhas sejam excluídos, porque a política de retenção no cofre local está definida como. `Retain` Ele preserva seus dados.

Próxima etapa: desligue AWS Backup sua landing zone

Depois que o pré-requisito for atendido ao desativar os backups do seu OUs, para desativar os backups do console do AWS Control Tower, navegue até a página de configurações da zona de pouso. Escolha Desativar backup.

Quando você desativa AWS Backup, o AWS Control Tower altera os seguintes recursos:

- Remove todos os conjuntos de pilhas relacionados a AWS Backup
- Desativa todos os controles relacionados à OU AWS Backup de segurança
- Cancela o registro da conta de administrador delegado para administração AWS Backup
- Remove a governança do AWS Control Tower (para CloudTrail AWS Config, e assim por diante) das contas do AWS Backup Administrador e do Backup Central

- O AWS Control Tower retém os AWS Backup cofres e os recursos do bucket Amazon S3 contendo seus dados

Depois de desativar os backups, nenhum novo backup será criado, mas os existentes não serão removidos.

Ativar backup em contas movidas

Se você mover uma conta para uma OU do AWS Control Tower que tenha sido AWS Backup ativada e a conta não estiver inscrita na AWS Control Tower, seu plano de backup não se aplicará automaticamente à conta.

Console: AWS Backup Para habilitar uma conta individual no console do AWS Control Tower, você pode escolher Atualizar conta na página de detalhes da conta ou pode escolher Registrar novamente a OU na página de detalhes da OU para atualizar várias contas ao mesmo tempo.

API: a partir da API, se você mover uma conta para uma OU que tenha a linha de base de backup ativada, poderá chamar a `ResetEnabledBaseline` API nessa OU, especificando o `EnabledBaseline` recurso da OU como destino, para acionar backups na conta por herança da OU.

Exemplo de comando:

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
 arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/XOSDORW8HDB5ZNWEE --region us-
east-1
```

Exemplo de resposta:

```
{
        "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

Desvio de backup no AWS Control Tower

O desvio não é relatado para AWS Backup configurações no AWS Control Tower. Para obter mais informações sobre desvios na AWS Control Tower, consulte Detectar e resolver desvios na AWS Control Tower.

Se você excluir ou modificar o AWS Backup plano, seu plano poderá entrar em um estado de desvio. Aqui estão algumas modificações a serem evitadas.

- Não mova a conta do Administrador de Backup da OU de Segurança.
- Não mova a conta do Backup Central da OU de Segurança.
- Não remova a conta do Administrador de Backup da organização.
- Não remova a conta do Backup Central da organização.
- Não desconecte, conecte ou atualize o AWS Backup SCP aplicado à OU de segurança.
- Não desconecte, conecte ou atualize o AWS Backup SCP aplicado a outros. OUs
- Não remova a permissão da conta do Administrador de Backup para AWS Backup.
- Não atualize suas configurações de backup entre contas para desativar os backups entre contas. Para obter mais informações sobre backups entre contas, consulte `UpdateGlobalSettings`a Referência da AWS Backup API.
- Não exclua sua AWS KMS chave.
- Não modifique sua política de AWS KMS chaves depois que ela for definida.
- Não desative o acesso confiável do serviço para AWS Backup.

> **Note**
>
> A deriva é relatada em relação ao status dos controles baseados em SCP que protegem os AWS Backup recursos no AWS Control Tower.

Recursos criados para AWS Backup

As tabelas nesta página mostram os recursos que são criados nas contas do AWS Control Tower quando você habilita AWS Backup.

A tabela a seguir mostra os recursos que o AWS Control Tower cria na conta do AWS Control Tower Central Backup quando você habilita AWS Backup a organização da landing zone.

Descrição	Recursos para a conta Central Backup
Qual OU contém a conta?	Segurança OU

Descrição	Recursos para a conta Central Backup
Qual ação criou o recurso?	Criação ou atualização da zona de pouso
Quais recursos são criados?	Cofre de Backup Central— `aws-controltower-central-backupvault-*`
Quais regiões estão incluídas?	Todas as regiões governadas
Quais controles estão relacionados a esses recursos?	`CT.BACKUP.PV.3`

A tabela a seguir mostra os recursos que o AWS Control Tower cria na conta do administrador de backup do AWS Control Tower quando você habilita AWS Backup a organização da landing zone.

Descrição	Recursos para a conta do Administrador de Backup: Essa é a conta de administrador delegado para AWS Backup
Qual OU contém a conta?	Segurança OU
Qual ação criou o recurso?	Criação ou atualização da zona de pouso
Quais recursos são criados?	Backup Audit Manager (BAM) • `aws_controltower_copy_report` • `aws_controltower_backup_report` • `aws_controltower_restore_report` Bucket Amazon S3 para armazenar registros do BAM— `aws-controltower-backup-reports-` *`{accountId}`* `-*` Bucket de registro de acesso ao Amazon S3— `aws-controltower-backup-reports-log-` *`{accountId}`* `-*`

Descrição	Recursos para a conta do Administrador de Backup: Essa é a conta de administrador delegado para AWS Backup
Quais regiões estão incluídas?	Região inicial
Quais controles estão relacionados a esses recursos?	• `CT.BACKUP.PV.2` • `CT.S3.PV.1` • `CT.S3.PV.1`

A tabela a seguir mostra os recursos que o AWS Control Tower cria na conta de auditoria da AWS Control Tower e na conta do AWS Control Tower Log Archive quando você habilita AWS Backup a OU de segurança.

Descrição	Recursos para contas de auditoria e arquivamento de registros
Qual OU contém a conta?	Segurança OU
Qual ação criou o recurso?	Ativando o `BackupBaseline`

Quais recursos são criados?	• Cofre de backup local— `aws-controltower-local-backupvault-*`
	• Função de Backup Local— `aws-controltower-BackupRole`
	• Quatro planos de Backup locais (por hora, semanalmente, mensalmente, diariamente)
	  • `aws-controltower-hourly-backup-plan`
	  • `aws-controltower-daily-backup-plan`
	  • `aws-controltower-weekly-backup-plan`
	  • `aws-controltower-monthly-backup-plan`

Descrição	Recursos para contas de auditoria e arquivamento de registros
	• Uma função do IAM— `aws-controltower-backup-role`
Quais regiões estão incluídas?	Todas as regiões governadas
Quais controles estão relacionados a esses recursos?	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

> **Note**
>
> Quando você aplica o `BackupBaseline` à OU de Segurança, todas as contas membros dessa OU recebem os AWS Backup recursos, não apenas as contas de Auditoria e Arquivamento de Registros.

A tabela a seguir mostra os recursos que o AWS Control Tower cria nas contas de membros da OU do AWS Control Tower quando você ativa AWS Backup em uma OU de destino.

Descrição	Recursos para contas de membros em outros OUs
Qual OU contém a conta?	Qualquer OU que não seja a OU de segurança
Qual ação criou o recurso?	Ativando o `BackupBaseline`
Quais recursos são criados?	• Cofre de backup local— `aws-controltower-local-backupvault-*` • Função de Backup Local— `aws-controltower-BackupRole` • Quatro planos de Backup locais (por hora, semanalmente, mensalmente, diariamente)

Descrição	Recursos para contas de membros em outros OUs
	• `aws-controltower-hourly-backup-plan` • `aws-controltower-daily-backup-plan` • `aws-controltower-weekly-backup-plan` • `aws-controltower-monthly-backup-plan` • Uma função do IAM— `aws-controltower-backup-role`
Quais regiões estão incluídas?	Todas as regiões governadas
Quais controles estão relacionados a esses recursos?	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

Controles para AWS backup

Quando você ativa AWS Backup na sua zona de pouso do AWS Control Tower, alguns controles preventivos são ativados em seu ambiente. Esses controles protegem os recursos que AWS Backup precisam operar com o AWS Control Tower. Você não pode ativar esses controles AWS Backup se não estiverem habilitados para sua landing zone.

Para obter mais informações, consulte Controles para AWS Backup.

Descomissione uma landing zone 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 pelo AWS Control Tower é chamado de desativação de uma zona de pouso.

Se você não quiser mais usar o AWS Control Tower, a ferramenta de desativação automática limpa os recursos alocados pelo AWS Control Tower. Para iniciar o processo de desativação automática, acesse a página Configurações de zona inicial, selecione a guia de desativação e escolha Desativar zona de pouso.

Consulte uma lista completa das ações executadas durante a desativação em Visão geral do processo de desativação.

> **Warning**
>
> Excluir manualmente todos os seus recursos do AWS Control Tower não é o mesmo que desativar. Isso não permitirá que você configure uma nova zona de pouso.

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 os buckets do Amazon S3 e os 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 desativação realizadas pelo AWS Control Tower e os artefatos que permanecem após a desativação são 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 desativação

Ao solicitar a desativação da zona de pouso, o AWS Control Tower realiza as ações a seguir.

- Desativa cada controle de detecção habilitado na zona de pouso. 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) de AWS Organizations. Se uma política estiver vazia (o que deveria acontecer depois de remover todas as políticas 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 realiza as seguintes ações durante o processo de desativação.
  - Exclui os registros de cada conta de fábrica de contas.
  - Revoga as permissões do AWS Control Tower para a conta removendo o perfil do IAM criado pelo AWS Control Tower (a menos que políticas complementares tenham sido adicionadas a ele) e recria o perfil `OrganizationsFullAccessRole` 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 (de auditoria e de arquivamento de logs).
- Revoga as permissões do AWS Control Tower das contas compartilhadas removendo o perfil do IAM criado pelo AWS Control Tower (a menos que políticas adicionais tenham sido adicionadas a ele) e recria o perfil do IAM `OrganizationsFullAccessRole`.
- Exclui registros relacionados às contas compartilhadas.
- Exclui registros relacionados aos criados pelo cliente OUs.
- 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.

Como desativar uma zona de pouso

Para descomissionar sua zona de pouso do AWS Control Tower do console, siga o procedimento fornecido aqui.

> **Note**
>
> Recomendamos que você cancele o gerenciamento de suas contas inscritas antes da desativação.

1. Acesse a página de Configurações de zona inicial no console do AWS Control Tower.
2. Escolha Desativar sua zona de pouso na seção Desativar sua zona de pouso.
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 confirmar sua intenção de desativar a zona de pouso, você será redirecionado para a página inicial do AWS Control Tower enquanto a desativação estiver em andamento. O processo pode exigir até duas horas.
5. Quando a desativação tiver sido concluída com êxito, você deverá excluir os recursos restantes manualmente antes de configurar uma nova zona de pouso 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 faturamento e conformidade. Por exemplo, a falha na 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. Insira o seguinte comando pela CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

Desative sua landing zone com APIs

O processo de limpeza de todos os recursos da zona de pouso é chamado de desativação 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 o AWS Control Tower lida com seus dados e os existentes AWS Organizations, revise. Descomissione uma landing zone do AWS Control Tower

Para desativar uma zona de pouso, chame a API `DeleteLandingZone`. Essa API retorna um `OperationIdentifier`, que você pode usar ao chamar a API `GetLandingZoneOperation` 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"
}
```

Tarefas de limpeza manual necessárias após a desativação

Esta seção lista as tarefas de limpeza manual que você deve executar após a etapa inicial de descomissionamento.

- Você deverá especificar endereços de e-mail diferentes para as contas de auditoria e de arquivamento de logs se criar uma zona de pouso após desativar uma, ou siga o procedimento para trazer suas próprias contas de auditoria e de arquivamento de logs.
- 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 logs 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 da UO de segurança do AWS Control Tower, você deve primeiro excluir as contas de auditoria e registro em log, mas não a conta de gerenciamento. Para excluir essas contas, você deve Quando fazer login como usuário-raiz 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 pelo AWS Control Tower e remover o conjunto de AWS CloudFormation pilhas associado.

- Antes de configurar um novo landing zone em uma nova AWS região, você deve seguir estas etapas adicionais.
  - Insira o seguinte comando pela 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.

Recursos não removidos durante a desativação

A desativação de uma zona de pouso 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.
- A Segurança e a Sandbox não OUs 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 Centro de Identidade do IAM, o AWS Control Tower configura o Centro de Identidade do IAM e configura um diretório inicial. Quando você desativa a zona de pouso, o AWS Control Tower não faz alterações no Centro de Identidade do IAM. Se necessário, você pode excluir manualmente as informações do Centro de Identidade do IAM armazenadas na 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 AWS contas e conjuntos de permissões do IAM Identity Center não são removidas.
- Os diretórios do Centro de Identidade do IAM não são alterados.
- Essas políticas do IAM Identity Center para o AWS Control Tower não foram removidas:
  - `AWSControlTowerAdminPolicy`
  - `AWSControlTowerCloudTrailRolePolicy`
  - `AWSControlTowerStackSetRolePolicy`

Perfis

Durante a configuração, o AWS Control Tower cria determinadas funções para você se você usar o console, ou solicita que você crie essas funções se você configurar sua landing zone por meio do APIs. Ao desativar a zona de pouso, os seguintes perfis não são removidos:

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

Buckets do Amazon S3

Durante a configuração, o AWS Control Tower cria buckets na conta de registro em log para registro em log e acesso de registro em log. 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 (de auditoria e de arquivamento de logs) são criadas na UO 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 encerradas.
- 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 AWS contas. 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 limpá-los encerrando-os, suas contas serão movidas para a UO raiz.
- A VPC que o AWS Control Tower criou não é removida, e o conjunto de pilhas associado do AWS CloudFormation (`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-membro, para todas as regiões administradas. A regra não é excluída automaticamente durante a desativação, então você deve excluí-la manualmente das contas compartilhadas e contas-membros de todas as regiões administradas antes de poder configurar uma zona de pouso em uma nova região.

Os procedimentos sobre como excluir recursos do AWS Control Tower são fornecidos em Remova os recursos do AWS Control Tower.

Remova 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 desativar a zona de pouso.

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 permaneceram após a desativação automatizada.

> **Warning**
>
> A remoção manual de recursos não permitirá que você configure uma nova zona de pouso. Não é o mesmo que desativação. Se você pretende desativar a zona de pouso do AWS Control Tower, siga as instruções em Descomissione uma landing zone do AWS Control Tower antes de realizar qualquer ação descrita neste capítulo. As instruções neste capítulo podem ajudar a limpar os recursos que restam após a conclusão da desativação automática.

Mesmo se excluir todos os recursos da zona de pouso manualmente, não será o mesmo que desativar a zona de destino e você poderá incorrer em cobranças inesperadas.

Se você precisar remover uma conta do AWS Control Tower, consulte as seções a seguir para encerrar uma conta:

- Unmanage an account
- Close an account created in Account Factory

Preciso desativar em vez de excluir?

Caso não pretenda mais usar o AWS Control Tower para sua empresa, ou caso precise de uma grande reimplantação de recursos organizacionais, talvez você queira desativar os recursos criados na configuração inicial da zona de pouso.

- 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 manualmente os recursos restantes nas contas antes de configurar outra zona de pouso, e para evitar a possibilidade de cobranças inesperadas. Para obter mais informações, consulte Recursos não removidos durante a desativação.

Warning

Recomendamos veementemente realizar esse processo de desativação somente se você pretende parar de usar a zona de pouso. 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 precisa excluir um recurso específico da zona de pouso.

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 desvios de governança na configuração do AWS Control Tower. Não podem ser desfeitos.

Tópicos

Excluir SCPs

O AWS Control Tower usa políticas de controle de serviço (SCPs) para seus controles. Este procedimento explica como excluir os itens SCPs especificamente relacionados ao AWS Control Tower.

Para excluir AWS Organizations SCPs

1. Abra o console Organizations em https://console.aws.amazon.com/organizations/.
2. Abra a guia Políticas e encontre as Políticas de Controle de Serviços (SCPs) que têm 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 da AWS conta IDs para 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 a AWS conta da IDs qual você fez um registro na etapa 3.b, separada 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 Stacks, pesquise todas as pilhas com o prefixo AWSControl Tower.

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).

Excluir buckets do Amazon S3 na conta de arquivamento de logs

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 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 Mudar de perfil.
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 Mudar de perfil.

Como 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 o produto e o portfólio do 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.

Como fazer login na conta de gerenciamento com as permissões certas

1. Acesse a URL do portal do usuário em *directory-id* .awsapps.com/start
2. Em Conta da AWS , encontre a conta de Gerenciamento.
3. Em AWSServiceCatalogAdminFullAccess, escolha Console de gerenciamento para entrar no AWS Management Console como esta função.

Como 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, procure um portfólio chamado Portfólio do Account Factory do AWS Control Tower.
4. Escolha o nome desse portfólio para acessar a página de detalhes.
5. Expanda a seção Restrições da página e escolha o botão de opção da restrição com o nome do produto Account Factory do AWS Control Tower.
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 opção do produto chamado Account Factory do AWS Control Tower.
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, procure um portfólio chamado Portfólio do Account Factory do AWS Control Tower.
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 Produtos de administrador, procure o produto chamado Account Factory do AWS Control Tower.
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).

Remover perfis e políticas do AWS Control Tower

Esses procedimentos mostram como limpar os perfis e as políticas que o AWS Control Tower criou quando a zona de pouso foi configurada ou posteriormente.

Para excluir a função do IAM Identity Center AWSService CatalogEndUserAccess

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 Contas da AWS .
4. Escolha o link da sua conta de gerenciamento.
5. Escolha a lista suspensa para Conjuntos de permissões AWSServiceCatalogEndUserAccess, selecione e escolha Remover.

6. Escolha Contas da AWS no painel à esquerda.
7. Abra a guia Permission sets (Conjuntos de permissões).
8. Selecione AWSServiceCatalogEndUserAccesse exclua.

Como excluir perfis do IAM

1. Abra o console do 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).

Como excluir políticas do IAM

1. Abra o console do 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 para 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.

Configuração após a desativação de uma zona de pouso

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 do AWS Control Tower faz parte da UO raiz do AWS Control Tower. Certifique-se de que esses perfis do IAM e políticas do IAM sejam removidas da conta de gerenciamento:
  - Perfis:
    - `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 configurar 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 trazer suas próprias contas de auditoria e de registro em log. Para obter mais informações, consulte Considerações sobre como trazer contas de segurança ou registro em log existentes.
- A configuração falhará se os buckets do Amazon S3 com os seguintes nomes reservados já existirem na conta de registro em log:
  - `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.

- Insira o seguinte comando pela CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Exclua a regra gerenciada restante, chamada `AWSControlTowerManagedRule`, das contas compartilhadas e contas-membros de todas as regiões administradas.

> **Note**
>
> Você não pode configurar uma nova landing zone em uma organização de nível superior OUs chamada Security ou Sandbox. Você deve renomeá-los ou removê-los OUs para configurar uma landing zone novamente.

Instruções

Este capítulo contém procedimentos de demonstração que podem ajudar você a usar o AWS Control Tower.

Tópicos

Demonstração: 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 zona de pouso, a AWS criou 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 migrar do ALZ para o 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 by Service Catalog APIs

O AWS Control Tower é integrado a vários outros AWS serviços, como AWS Service Catalog. Você pode usar o 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, ligando para AWS Service Catalog APIs o. 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 do ambiente de desenvolvimento do AWS Cloud9 para execução desse 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 tiver familiaridade com o Terraform, você poderá provisionar contas com o Account Factory for Terraform (AFT) do AWS Control Tower.

Exemplo de perfil de administração de automação

Aqui está um exemplo de modelo que você pode usar para ajudar a configurar o perfil de administração de automação na conta de gerenciamento. Esse perfil deveria ser configurado 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 perfil de execução de automação

Aqui está um modelo de exemplo que você pode usar para ajudar a configurar a função de execução de automação. Esse perfil deveria ser configurado 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 o 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 do Service Catalog

Aqui está um exemplo da entrada que você pode fornecer à API do Service Catalog se estiver usando a API `ProvisionProduct` 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"
}
```

Consulte mais informações na Referência de APIs 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.

Vídeo de demonstração

Este vídeo (6:58) descreve como automatizar implantações de conta 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.

Video Walkthrough of Automated Account Provisioning in AWS Control Tower.

Demonstração: configure o AWS Control Tower sem uma VPC

Este tópico descreve como configurar suas contas do AWS Control Tower sem uma VPC.

Se a sua workload não exigir uma VPC:

- Você poderá excluir a nuvem privada virtual (VPC) do AWS Control Tower. Essa VPC foi criada ao configurar sua zona de destino.
- Você poderá 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 habilitadas, essa configuração do Account Factory substituirá o controle Proibir o acesso à internet para uma instância da Amazon VPC gerenciada por um cliente. Para evitar a habilitação do acesso à internet para contas recém-provisionadas, você deve alterar a configuração no Account Factory.

Excluir 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 é associada à conta de gerenciamento do AWS Control Tower. Este tópico refere-se a essa nova VPC como a VPC do Control Tower.

Ao visualizar a VPC do AWS Control Tower no console da Amazon VPC, você não verá a palavra (padrão) no final do nome. Se tiver mais de uma VPC, você deverá usar o intervalo CIDR atribuído para identificar a VPC correta do AWS Control Tower.

É possível excluir a VPC do AWS Control Tower, mas se você precisar de uma VPC no AWS Control Tower posteriormente, deverá criá-la por conta própria.

Como excluir a VPC do AWS Control Tower

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. Procure **VPC** ou selecione VPC nas opções do Service Catalog. Será exibido o VPC Dashboard (Painel da VPC).
3. No menu à esquerda, escolha Seu VPCs. Em seguida, você verá uma lista de todos os seus VPCs.
4. Identifique a VPC do AWS Control Tower por seu intervalo 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, além de remover a VPC criada pelo Control Tower na região de origem do AWS Control Tower.

Opcionalmente, limpe o recurso VPC na conta

Opcionalmente, para limpar o recurso de VPC do AWS Control Tower`aws-controltower-VPC`, de uma conta existente, você pode remover a instância de pilha AWS CloudFormation StackSet `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1` da, depois de se certificar de que não há recursos ou dependências de recursos existentes na VPC.

Criar uma conta no AWS Control Tower sem uma VPC

Se suas cargas de trabalho de usuário final não exigirem VPCs, você pode usar esse método para configurar contas de usuário final que não foram VPCs criadas automaticamente para eles.

No painel do AWS Control Tower, é possível visualizar e editar suas definições de 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 serão 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. Será exibida a página do 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: remover 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 AWS Control Tower VPC ou reconfigura o Account Factory para criar contas sem ela. VPCs

- A conta de gerenciamento existente pode ter dependências ou recursos na VPC do 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 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 configurar políticas de segurança e impor regras de segurança para suas organizações do AWS Control Tower, e como corrigir recursos não compatíveis aplicando políticas automaticamente. Você pode visualizar os grupos de segurança que estão em vigor para cada conta e recurso (como uma EC2 instância da Amazon) 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 segurança da infraestrutura de rede melhor para seus recursos e workloads 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.

Video Walkthrough of Firewall Setup in AWS Control Tower.

Consulte mais informações na documentação sobre como configurar o AWS WAF.

Solução de problemas

Se enfrentar problemas ao usar o AWS Control Tower, você poderá usar as informações a seguir para resolvê-los de acordo com nossas práticas recomendadas. Se os problemas enfrentados estiverem fora do escopo das informações a seguir ou se eles persistem depois que você tiver tentado 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 a conta de gerenciamento tiver menos de uma hora de criação, você poderá enfrentar problemas quando as contas adicionais forem criadas.

Ação a realizar

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 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 ser 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.

Ação a realizar

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 o AWS Control Tower.

Erro de zona de pouso não atualizada

Se não atualizou a zona de pouso recentemente, você pode receber uma mensagem de erro ao tentar recuperar o acesso ao AWS Control Tower. Você pode receber 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 a zona de pouso para acessar o AWS Control Tower.

No entanto, a atualização da zona de pouso pode falhar.

Etapas a realizar

Faça login na conta de gerenciamento da organização e faça login como usuário-raiz. Seu usuário do IAM ou usuário no IAM Identity Center deve ter permissões de administrador do AWS Control Tower e fazer parte do AWSControlTowerAdminsgrupo. Depois, 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 obter 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.
- Ocorrerá uma falha na criação de uma conta no Account Factory enquanto são feitas outras alterações de configuração do AWS Control Tower. Por exemplo, durante um processo para

adicionar um controle a uma UO, o Account Factory exibirá uma mensagem de erro se você tentar provisionar uma conta.

Como 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 Depois, é necessário usar o console do AWS Organizations para mover manualmente a conta para fora da UO e de volta 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. O AWS Control Tower tem sua própria VPC padrão que substitui a VPC padrão da AWS , a menos que você configure o Account Factory da maneira que o passo a passo mostra, para que o 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 realizar: você deve excluir a VPC padrão adicionada e, depois, conseguirá atualizar a conta.

> **Note**
>
> O estado `Tainted` causa um problema subsequente: uma conta não atualizada pode impedir a habilitação de controles na UO da qual faz parte.

Caso 2: você pode receber 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 realizar:

Se a mudança de conta foi planejada:

- Encerre a conta no Service Catalog.

- Inscreva-a 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 de conta não foi planejada:

- Retorne a conta para sua UO original.
- Atualize a conta no Service Catalog.
- Nos parâmetros de inicialização, insira a UO na qual a conta estava originalmente.
- Contexto/impacto: se a conta não retornar à UO original, seu estado será inconsistente com os controles ditados pela nova UO em que ela está.
- Atualizar uma conta não é uma correção válida, pois não exclui as regras do AWS Config associadas à UO anterior.

Não é possível atualizar a zona de pouso

O AWS Control Tower não reverterá para uma versão anterior da zona de pouso se uma atualização falhar. Você pode encontrar a zona de pouso 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 cumpridos
- AWS Config existem recursos em determinadas contas
- Existem contas encerradas

Pré-requisitos não cumpridos

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 zona de pouso não pode ser concluído com esses recursos presentes. Essas restrições são semelhantes às de inscrever uma conta ou configurar uma zona de pouso pela primeira vez. Para obter mais informações, consulte Inscrever contas que tenham AWS Config recursos existentes.

Existem contas encerradas

Quando uma conta está no estado Encerrada ou Suspensa, você pode encontrar um problema ao tentar atualizar a zona de pouso. Você deve excluir o produto provisionado em cada conta encerrada antes de realizar uma atualização na zona de pouso.

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 realizar: caso veja 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 realizar: 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, tente iniciar o AWS Control Tower novamente 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 receber 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)
- Managing the Delivery Channel

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 ter feito login como raiz. O AWS Control Tower não permite criar contas quando você faz login como usuário-raiz.
- Seu usuário do Centro de Identidade do IAM não foi adicionado ao grupo de permissões apropriado. Talvez seja necessário adicionar seu usuário do IAM Identity Center a um desses grupos de permissões: 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 ocorrerá se você tiver as permissões corretas, mas o desvio do AWS Control Tower for detectado e for necessário repará-lo. Para reparar a maioria dos tipos de desvio, escolha Redefinir na página Configurações de zona inicial.

Recebeu um erro de permissões insuficientes

É possível que a conta não tenha as permissões necessárias para executar determinado trabalho em determinado AWS Organizations. Se você encontrar o seguinte tipo de erro, verifique todas as áreas de permissões, como permissões do IAM ou do Centro de Identidade do IAM, para garantir que a permissão não está sendo negada destes locais:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Se você acredita que seu trabalho requer a ação que está tentando e não consegue localizar nenhuma restrição relevante, entre em contato com o administrador do sistema ou o com o AWS Support.

Os controles de detecção não estão 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 OUs regidas pela AWS Control Tower sejam atualizadas. Os controles de detecção existentes em contas existentes ainda estão em vigor.

Se você tentar habilitar um controle de detecção antes de atualizar suas contas, poderá receber 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 pelo console do AWS Control Tower, consulte Quando atualizar a AWS Control Tower OUs e as contas.

Para atualizar várias contas individuais de forma programática, você pode usar o formulário AWS Service Catalog e APIs a AWS CLI para automatizar as atualizações. Para obter mais informações sobre como abordar o processo de atualização, consulte Vídeo de demonstração. Você pode substituir a UpdateProvisionedProductAPI pela ProvisionProductAPI mostrada no vídeo.

Se você tiver mais dificuldades em habilitar os controles de detecção nas 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 SCPs você estava à deriva.

Etapas a seguir

Se você encontrar um erro de `rate exceeded` ou controle de utilização de API, siga estas etapas:

- Execute suas workloads em um horário diferente. (Consulte o cronograma de verificação de invariância da SCP do AWS Control Tower por região para descobrir quando o AWS Control Tower executa suas verificações de auditoria.)
- Se você estiver chamando o APIs diretamente por meio de HTTP: use o AWS SDK, que repete automaticamente as ações com falha
- Solicitar um aumento de limite por meio do Service Quotas e do AWS Support

Um exemplo de instruções de solução de problemas para controle de utilização 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 do AWS Control Tower para outra

> **Warning**
>
> Essa prática não atende ao pré-requisito para a inscrição de contas elegíveis, porque elas devem fazer parte do mesmo AWS Organization, e cada organização pode ter apenas uma zona de pouso. Se você tentou realizar 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 zona de pouso gerenciada pelo AWS Control Tower, em outra conta de gerenciamento, é necessário remover todos os perfis do IAM e as pilhas associadas a essa conta da UO 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 UO original antes de tentar movê-la.

Se você não remover os recursos, a inscrição na nova UO falhará inevitavelmente. Você pode encontrar uma ou mais mensagens de erro e continuará recebendo mensagens semelhantes até que os perfis e as 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 UO, excluir o recurso antigo que é o assunto da mensagem de erro e tentar mover a conta de volta para a nova UO. 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 UO com uma SCP que impede a exclusão do perfil 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 poderá receber se os perfis e as pilhas não excluídas permanecerem. Você provavelmente receberá uma dessas mensagens por vez, sempre que tentar registrar a conta, desde que os recursos antigos permaneçam.

Os valores das strings 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 receber uma mensagem semelhante a estes 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 receber 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 UO, você poderá convidar, provisionar ou inscrever a conta na nova UO com sucesso.

AWS Support

Se pretender mover as suas contas-membros 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 destino. O destino da linha de base mais comum pode ser uma unidade organizacional (UO). Por exemplo, é possível habilitar uma linha de base com uma UO selecionada como destino para registrar essa UO no AWS Control Tower.

Durante a configuração da zona de pouso, o destino de linha de base 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 definições e configurações de zona inicial. 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 dois tipos gerais de linhas de base:

- Tipos de linha de base que podem ser aplicados a uma OU registrada no AWS Control Tower ou a uma OU que você pretende registrar aplicando a linha de base.
- Tipos de linha de base que podem ser aplicados a uma zona de pouso ou conta compartilhada, durante a configuração inicial ou durante uma atualização da zona de pouso.

Tipos de linha de base que se aplicam no nível da OU, para registro e atualização OUs

- Nome: `AWSControlTowerBaseline`

  Descrição: configura recursos e controles obrigatórios para contas-membros dentro da UO de destino, necessários para a governança do AWS Control Tower.

  Consideração: essa linha de base mantém as configurações do controle de Negação de região da zona de pouso. Em outras palavras, se uma região não é permitida no nível da zona de pouso, essa região não é permitida para aquela UO quando você chama a API `EnableBaseline` para registrar uma UO.

> **Note**
>
> O controle de negação de região no nível da UO não tem como permitir regiões que o controle de negação de região da zona de pouso não permite.

Para obter mais informações, consulte Como SCPs trabalhar com a negação na AWS Organizations documentação.

Recomendação: recomendamos que você confirme as regiões nas quais a UO de destino pode estar executando workloads e verifique os resultados em relação ao controle de negação de região da zona de pouso, antes de chamar a API `EnableBaseline` para a OU. Caso contrário, você poderá perder o acesso a recursos em determinadas regiões.

- Nome: `BackupBaseline`

  Descrição: Essa linha de base configura recursos e controles para contas de membros na OU de destino. Eles são necessários para que a integração com o AWS Backup possa automatizar seu backup de dados e centralizar o gerenciamento de suas políticas de backup. Serviços da AWS

  Consideração: Antes de habilitar o `BackupBaseline` em uma OU de destino, certifique-se de que `AWSControlTowerBaseline` esteja habilitado na OU de destino. Ou seja, a OU de destino deve estar registrada no AWS Control Tower.

  - Você pode optar por ativar AWS Backup durante o processo de criação da sua zona de pouso do AWS Control Tower ou durante um processo de atualização da zona de pouso.
  - `BackupBaseline`É compatível com as versões 3.1 e posteriores do landing zone.
  - O não `BackupBaseline` é aplicado à conta de gerenciamento.

> **Note**
>
> As linhas de base da zona de pouso se comportam de maneira diferente das linhas de base do nível da UO.

Tipos de linha de base que podem se aplicar à zona de pouso ou contas compartilhadas

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 zona de pouso podem mudar conforme você altera as configurações de zona inicial. Por exemplo, se você optar pelo Centro de Identidade do IAM, o AWS Control Tower poderá habilitar a versão mais recente da linha de base `IdentityCenterBaseline` na zona de pouso.

Você pode ver as linhas de base habilitadas para a zona de pouso com a chamada de API `ListEnabledBaselines`.

> **Note**
>
> Somente o `AWSControlTowerBaseline` pode ser aplicado diretamente com a `EnableBaseline` API. Outras linhas de base são gerenciadas automaticamente (`AuditBaseline`,`LogArchiveBaseline`). O status de `IdentityCenterBaseline` é fornecido como informação quando você aplica `AWSControlTowerBaseline` o.

- Nome: `AuditBaseline`

  Descrição: configura recursos para monitorar a segurança e a conformidade das contas em sua organização. Não é possível alterar essa linha de base. Ela é implantada pelo AWS Control Tower.
- Nome: `LogArchiveBaseline`

  Descrição: configura um repositório central para logs de atividades de API e configurações de recursos de contas em sua organização. Não é possível alterar essa linha de base. Ela é implantada pelo AWS Control Tower.
- Nome: `IdentityCenterBaseline`

  Descrição: configura recursos compartilhados para o Centro de Identidade do IAM, que prepara o `AWSControlTowerBaseline` para configurar o acesso ao Centro de Identidade para contas.

  Consideração: essa linha de base funciona somente quando você seleciona o Centro de Identidade do IAM como seu provedor de identidades no momento em que configurou a zona de pouso inicialmente, ou se você altera mais tarde as configurações de zona inicial para habilitar

o Centro de Identidade do IAM para a zona de pouso. Se você estiver usando um provedor de identidades diferente, não terá acesso para habilitar essa linha de base.

- Nome: `BackupCentralVaultBaseline`

  Descrição: Configura o AWS Backup cofre central em sua organização.

- Nome: `BackupAdminBaseline`

  Descrição: configura o administrador delegado e o AWS Backup Audit Manager.

Inscrição parcial de contas

Quando você trabalha com linhas de base, uma conta pode ser colocada em um estado chamado Parcialmente inscrita.

Esse estado pode ocorrer se você registrar novamente uma UO chamando a API `ResetEnabledBaseline`, porque o AWS Control Tower aplica somente os recursos obrigatórios às contas na UO de destino. Uma conta que não tem os recursos opcionais (controles) da UO principal é marcada como Parcialmente inscrita.

Se você mover uma conta não inscrita para uma UO registrada e, depois, chamar a API `ResetEnabledBaseline` na UO para inscrever essa conta, o AWS Control Tower aplicará os recursos associados a `AWSControlTowerBaseline` à conta recém-inscrita. No entanto, os controles opcionais habilitados para essa UO não são aplicados à conta. A conta permanece em um estado Parcialmente inscrita.

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 UO à conta recém-inscrita, incluindo os controles opcionais que são ativados para essa UO.

Variação nas operações entre o console do AWS Control Tower e as APIs 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 quatro APIs linhas de base.

Diferenças

- Registro e produtos provisionados

  Ao registrar uma UO por meio do console, o AWS Control Tower cria produtos do Service Catalog para as contas-membros da UO, como parte da inscrição de cada conta. Quando você registra uma UO por meio da API `EnableBaseline` e `AWSControlTowerBaseline`, o AWS Control Tower não cria produtos provisionados para as contas-membros na UO.

- Cancelar o registro de uma UO

  Sempre que você cancelar o registro de uma OU, primeiro remova todas as contas de membros e as aninhadas. OUs Depois, o AWS Control Tower remove todos os controles que são aplicados à UO.

  - Se você selecionar Excluir UO para a UO do console, o AWS Control Tower cancelará o registro e, depois, excluirá a UO da sua organização.
  - No entanto, se você cancelar o registro da UO chamando a API `DisableBaseline` para remover `AWSControlTowerBaseline` da UO, o AWS Control Tower não excluirá a UO da organização, a UO ainda estará presente na organização, sem registro.

Linhas de base e padrões de versionamento

Se a zona de pouso do AWS Control Tower já estiver configurada e você optar por habilitar uma linha de base da zona de pouso, o AWS Control Tower habilita a versão mais recente da linha de base compatível com a versão da zona de pouso. Se você optar por habilitar uma linha de base para uma UO que ainda não esteja registrada no AWS Control Tower, o AWS Control Tower fornecerá automaticamente a versão mais recente compatível da linha de base para essa UO.

Compatibilidade das linhas de base da UO e das versões da zona de pouso

As linhas de base do AWS Control Tower permitem que você defina um padrão de governança no nível da UO, em vez de no nível da zona de pouso, se a sua empresa exigir. A linha de base chamada `AWSControlTowerBaseline` está disponível para ajudar a registrar você no OUs AWS Control Tower.

> **Note**
>
> Uma linha de base é um grupo de controles e recursos que funcionam em conjunto para estabelecer um ambiente de governança estável na zona de pouso.

Ao habilitar uma linha de base em uma UO, chamando a API `EnableBaseline` no AWS Control Tower, é necessário especificar uma versão de base que seja compatível com a versão atual da zona de pouso do AWS Control Tower. Depois de especificar uma linha de base, todas as contas-membros em uma UO seguem a linha de base fornecida para a UO. Em outras palavras, novas contas são provisionadas com a linha de base atualizada e as contas-membros existentes são governadas de acordo com a nova linha de base.

Se você não selecionar uma linha de base para suas contas OUs e contas existentes, a versão landing zone determinará toda a postura de governança, por padrão. No entanto, cada UO registrada na zona de pouso recebe uma versão da linha de base, que é a mais recente compatível com a versão atual da zona de pouso. Portanto, cada UO e conta-membro inscrita tem uma linha de base associada, mesmo que você nunca atribua uma linha de base especificamente.

Para a linha de base no nível da 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 da linha de base	Versões da zona de pouso	Esquemas incluídos	Controles incluídos	Alteração em relação à linha de base anterior	
1,0	De 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 da linha de base	Versões da zona de pouso	Esquemas incluídos	Controles incluídos	Alteração em relação à linha de base anterior	
		NE_SERVIC E_ROLES, recursos do IAM			
2,0	De 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, SLR do Config, 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 da linha de base	Versões da zona de pouso	Esquemas incluídos	Controles incluídos	Alteração em relação à linha de base anterior	
3.0	De 3.0 a 3.1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, SLR do Config, recursos do IAM	Todos os controles obrigatórios	Novo AWS Config projeto. Alteração para recursos globais de registro somente na região de origem. CloudTrail Projeto removido	

Versão da linha de base	Versões da zona de pouso	Esquemas incluídos	Controles incluídos	Alteração em relação à linha de base anterior	
4,0	De 3.2 a 3.3	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, SLR do Config, recursos do IAM	Todos os controles obrigatórios	Novo esquema do SLR	

Consulte mais informações sobre recursos específicos criados em contas ao configurar a zona de pouso em Resources created in the shared accounts.

Se você atualizar a zona de pouso para uma versão compatível com uma versão mais recente da linha de base `AWSControlTowerBaseline`, e a nova versão da zona de pouso for compatível com sua versão de linha de base existente, o estado da UO mudará para Atualização disponível.

- É possível continuar usando a fábrica de contas e outros recursos sem atualizar a linha de base da UO imediatamente, exceto no caso de uma atualização da zona de pouso de 2.x para 3.x.
- As novas contas inscritas nessa UO recebem recursos com base na versão de linha de base existente até que ela seja atualizada (com o recurso de Governança estendida no console ou por meio da API `UpdateEnabledBaseline`).

- Depois de atualizar a versão da linha de base, todas as contas dentro dessa UO recebem recursos com base na nova versão da 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 da sua OUs, devido à mudança de trilhas em nível de conta para trilhas em nível de organização. AWS CloudTrail No console, a UO mostrará o status de Atualização necessária.

Considerações sobre as linhas de base

- Se a UO exigir uma atualização da linha de base, você não poderá provisionar novas contas nem inscrever contas existentes nessa UO.
- Depois de uma atualização da zona de pouso, se você também planeja atualizar uma linha de base de UO, será necessário registrar novamente a UO ou atualizar a versão da linha de base da UO programaticamente.
- Recomendamos que você atualize para a linha de base mais compatível com a versão da zona de pouso que está usando, para ter acesso a todos os benefícios da zona de pouso e da linha de base combinadas. Por exemplo, se atualizar para a versão 3.3 da zona de pouso, você ainda poderá usar a linha de base 3.0, mas não terá 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 habilitação da linha de base se destina a uma UO por vez. Portanto, os aninhados não OUs são atualizados automaticamente quando a OU principal é atualizada. Recomendamos que você atualize a OU principal antes de atualizar a aninhada OUs.
- Quando você chama a API `UpdateEnabledBaseline` ou registra novamente uma UO no console, a UO retém todos os controles que foram habilitados 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 com APIs apenas

Este demonstração de exemplos é um documento complementar. Consulte explicações, advertências e mais informações em Tipos de linhas de base.

Pré-requisitos

É necessário ter uma UO existente que não esteja registrada no AWS Control Tower e que você gostaria de registrar. Ou você deve ter uma UO registrada que gostaria de registrar novamente para fins de atualização.

Registrar uma UO

1. Verifique se `IdentityCenterBaseline` está habilitado para a zona de pouso. Em caso afirmativo, obtenha o identificador de linha de base habilitado para o Centro de Identidade.

```
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 do 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 de `AWSControlTowerBaseline`.

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Crie a linha de base de `AWSControlTowerBaseline` na UO de destino.

   Se a linha de base do Centro de Identidade estiver habilitada:

```
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 Centro de Identidade não estiver habilitada, omita o sinalizador *parameters*, da seguinte forma:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Registrar novamente uma UO

Depois de fazer atualizações nas configurações da zona de pouso ou atualizar sua versão da zona de pouso, você deve se registrar novamente OUs para fornecer as alterações mais recentes. Siga estas etapas para registrar novamente uma UO programaticamente, redefinindo o recurso `EnabledBaseline` associado.

1. Obtenha o ARN da UO de destino para registrar novamente.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Obtenha o ARN do recurso `EnabledBaseline` para a UO de destino.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. Redefina a linha de base habilitada.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

Exemplos de uso da API de linha de base

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 operação de API, consulte DisableBaseline.

Entrada de DisableBaseline:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

Saída de DisableBaseline:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

Exemplo da CLI de DisableBaseline:

```
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 operação de API, consulte EnableBaseline.

Entrada de EnableBaseline:

```
{
    "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"
```

```
        }
    ]
}
```

Saída de `EnableBaseline`, retornando um novo recurso:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

Exemplo da CLI de `EnableBaseline`:

Este exemplo mostra como habilitar uma linha de base para uma AWS Organizations organização que tem a landing zone ativada para acessar o AWS IAM Identity Center, gerenciado pelo AWS Control Tower. Para recuperar seu identificador `EnabledBaseline` do Centro de Identidade, chame a API `ListEnabledBaselines`, filtrando pela linha de base do Centro de Identidade: `(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 detalhe `EnabledBaseline`, 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 valor do ARN da resposta e passe esse valor como um parâmetro para habilitar 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 zona de pouso excluída do gerenciamento do AWS Control Tower do Centro de Identidade do IAM, habilite 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 operação de API, consulte GetBaseline.

Entrada de `GetBaseline`:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

Saída de `GetBaseline`:

```
{
    "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.",
}
```

Exemplo da CLI de `GetBaseline`:

```
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 operação de API, consulte GetBaselineOperation.

Entrada de `GetBaselineOperation`:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

Saída de `GetBaselineOperation`:

```
{
    "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"
    }
}
```

Exemplo da CLI de `GetBaselineOperation`:

```
aws controltower get-baseline-operation \
```

```
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

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

Entrada de `GetEnabledBaseline`:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

Saída de `GetEnabledBaseline`:

```
{
    "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"
            }
        ]
    }
}
```

Exemplo da CLI de `GetEnabledBaseline`:

```
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 operação de API, consulte ListBaselines.

Entrada de `ListBaselines` (usando entradas opcionais):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

Saída de `ListBaselines`:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-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-east-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-east-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."
        },
```

```
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9AOMU2",
            "name": "BackupCentralVaultBaseline",
            "description": "Sets up central AWS Backup vault in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
            "name": "BackupManagerBaseline",
            "description": "Sets up delegated admin and AWS Backup Audit Manager."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/APO9ATVPBKFRRGLK",
            "name": "BackupBaseline",
            "description": "Sets up local Backup vault and attach Backup policy."
        }
    ]
}
```

Exemplo da CLI de `ListBaselines`:

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

A `ListEnabledBaselines` API tem um parâmetro opcional que permite que você visualize as linhas de base conforme elas se aplicam às contas que são membros de uma OU. Os exemplos a seguir mostram alguns comandos da CLI que você pode usar para visualizar as linhas de base de uma conta. O AWS Control Tower se refere a essas linhas de base, que são habilitadas na OU, mas se aplicam a cada conta dentro da OU, como linhas de base habilitadas para crianças, porque elas derivam sua configuração de governança das linhas de base que são aplicadas na OU.

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

`ListEnabledBaselines`entrada para mostrar linhas de base habilitadas para crianças:

```
aws controltower list-enabled-baselines --include-children
```

`ListEnabledBaselines`saída para visualizar as linhas de base habilitadas para crianças:

```
{
```

```
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XO2UQ1PC6BB5085S5",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "statusSummary": {
                "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/
ou-k86y-1d9k8vpu"
        },
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XAFPKQQXOJB50ZWQH",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:666355521292:enabledbaseline/XOIZ4G08CWB50ZWON",
            "statusSummary": {
                "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:account/o-
vaex10vaey/183295447314"
        }
]
```

> **Note**
>
> No exemplo anterior, o `parentIdentifier` campo mostra a linha de base ativada da OU principal para essa linha de base habilitada para crianças.

Visualize todas as linhas de base aplicadas em um alvo específico (OU ou conta):

```
aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["TARGET_ARN"]
```

```
    }
```

Veja todos os OUs que têm uma linha de base específica:

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'
```

Veja todas as contas OUs e contas que têm uma linha de base específica:

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'  \
    --include-children
```

Visualize todas as contas em uma OU que tenham a Linha de Base B ativada:

```
### First fetch the enabled baseline record for Baseline B on the OU
 aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["OU_TARGET_ARN"],
        "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
    }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
 enabled baseline record on the OU
aws controltower list-enabled-baselines \
    --filter '{
        "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
    }' \
    --include-children
```

Mais sobre linhas de base habilitadas para crianças

- Você pode usar a `GetEnabledBaseline` API para visualizar informações detalhadas sobre uma linha de base específica habilitada para crianças
- Você pode usar a `GetBaselineOperation` API para visualizar uma operação realizada na linha de base habilitada para crianças.

- Você não pode chamar diretamente nenhuma gravação APIs, comoEnableBaseline,, ResetEnabledBaseline ou UpdateEnabledBaselineDisableBaseline, em uma linha de base habilitada para crianças.
- Os recursos básicos habilitados para crianças podem ser modificados somente por meio do serviço AWS Control Tower, por meio de operações que são realizadas na OU principal ou por meio do Account Factory.

Exemplos de uso de filtros:

Entrada de ListEnabledBaselines (sem filtros):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

Entrada ListEnabledBaselines (somente filtro baselineIdentifiers):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

Entrada ListEnabledBaselines (somente filtro targetIdentifiers):

```
{
    "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
}
```

Entrada de `ListEnabledBaselines` (filtros `baselineIdentifiers` e `targetIdentifiers`):

```
{
    "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
}
```

Saída de `ListEnabledBaselines`:

```
{
    "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"
}
```

Exemplo de CLI com um tipo de filtro (filtro `baselineIdentifiers`):

```
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
```

Exemplo de CLI usando vários filtros (filtros `baselineIdentifiers` e `targetIdentifiers`):

```
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 operação de API, consulte ResetEnabledBaseline.

Entrada de `ResetEnabledbaseline`:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

Saída de `ResetEnabledBaseline`:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

Exemplo da CLI de `ResetEnabledBaseline`:

```
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 operação de API, consulte UpdateEnabledBaseline.

Entrada de `UpdateEnabledBaseline`:

```
{
    "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"
        }
    ]
}
```

Saída de `UpdateEnabledBaseline`:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

Exemplo da CLI de `UpdateEnabledBaseline`:

```
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
```

Mais informações e links

Este tópico inclui links para publicações de blog relevantes, documentação técnica e informações relacionadas que podem ajudar você a trabalhar com o AWS Control Tower. As fontes abrangem alguns casos de uso comuns e as práticas recomendadas para os recursos do AWS Control Tower, além de alguns aprimoramentos adicionais.

Tutoriais e laboratórios

- Laboratório do AWS Control Tower: esses laboratórios oferecem uma visão geral de alto nível das tarefas comuns relacionadas ao AWS Control Tower.
- No painel do 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 do 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 Arquitetura VPC 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 recursos personalizados VPCs.
- Implementing Serverless Transit Network Orchestrator (STNO) in AWS Control Tower: essa publicação do blog demonstra como automatizar o acesso à conectividade de rede entre contas. Esse blog é destinado aos administradores do AWS Control Tower ou aos responsáveis pelo gerenciamento de redes no ambiente da AWS .

Segurança, identidade e registro em log

Amplie seu procedimento de segurança, integre-se com provedores de identidade externos ou existentes e centralize os sistemas de registro em log.

Segurança

- Automatização de AWS Security Hub alertas com eventos do ciclo de vida do AWS Control Tower — Esta postagem do blog descreve como automatizar a ativação e a configuração do Security Hub em um ambiente multicontas do AWS Control Tower em contas novas e existentes.
- Habilitando AWS Identity and Access Management — Esta postagem do blog descreve como aprimorar sua visibilidade de segurança organizacional ativando e centralizando as descobertas do IAM Access Analyzer.
- O AWS Systems Manager Parameter Store oferece armazenamento hierárquico seguro para o 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 pela 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 à 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 AWS Control Tower.

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.
- Para obter informações sobre como visualizar seus AWS Config recursos, consulte o Config Resource Compliance Dashboard.

Implantação de recursos e gerenciamento de workloads

Implante e gerencie recursos e workloads.

- Getting Started Library integration: essa publicação do blog descreve os portfólios de conceitos básicos que você pode usar.
- Continuous deployment of Cloud Custodian to AWS Control Tower

Trabalhar com organizações e contas existentes

Trabalhe com AWS organizações e contas existentes.

- Inscrever uma conta — Este tópico do guia do usuário descreve como inscrever uma AWS conta existente no AWS Control Tower.
- Coloque uma conta na AWS Control Tower — Esta postagem do blog descreve como implantar a AWS Control Tower em suas AWS organizações existentes.
- Extend AWS Control Tower governance using AWS Config conformance packs: essa publicação do blog descreve como implantar pacotes de conformidade do AWS Config para ajudar a colocar contas e organizações existentes na governança pelo AWS Control Tower.
- How to Detect and Mitigate Guardrail Violation with AWS Control Tower: essa publicação do blog descreve como adicionar controles e como assinar notificações do SNS para que você possa receber notificações por e-mail sobre violações de conformidade de controle.

Automação e integração

Automatize a criação de contas e integre eventos de ciclo de vida com o AWS Control Tower.

- Lifecycle events: essa publicação do blog descreve como usar eventos de ciclo de vida com o AWS Control Tower.
- Automate account creation: essa publicação do blog descreve como configurar a criação automática de contas no AWS Control Tower.
- Amazon VPC flow log automation: essa publicação do blog descreve como automatizar e centralizar logs de fluxo da Amazon VPC em um ambiente com várias contas.

- Automatize a marcação de VPC com eventos de ciclo de vida da AWS Control Tower — Esta postagem do blog descreve como automatizar a marcação VPCs de recursos por meio de eventos de ciclo de vida na AWS Control Tower.
- Automated account management: essa publicação do blog descreve como automatizar as tarefas de gerenciamento de contas após a configuração do ambiente do AWS Control Tower.

Migrar workloads

Use outros AWS serviços com o AWS Control Tower para ajudar 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

O AWS Control Tower atua como uma camada de orquestração para o AWS Organizations. Portanto, por meio do console do AWS Organizations APIs, você tem acesso a mais de 20 outros serviços da AWS que funcionam com o AWS Control Tower. Esses serviços adicionais não são acessíveis diretamente pelo console do AWS Control Tower.

- Consulte uma lista completa dos serviços disponíveis para o AWS Control Tower por meio do AWS Organizations em AWS services that you can use with AWS Organizations.
- Para habilitar recursos de várias contas para esses serviços relacionados da AWS, é necessário habilitar o acesso confiável. Para obter mais informações, consulte Usando o AWS Organizations com outros serviços da AWS.

  > **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. Não é necessário modificar as configurações de acesso confiável ou administração delegada para esses serviços.

- Alguns AWS serviços disponíveis por meio de administração delegada AWS Organizations podem usar administração delegada, incluindo o AWS Systems Manager e o AWS Firewall Manager. Consulte mais informações em Configuring a Delegated Administrator e em Enabling a delegated

administrator account for Firewall Manager. Veja também este vídeo: Set up security groups with AWS Firewall Manager.

AWS Marketplace soluções

Descubra soluções de AWS Marketplace.

- AWS Control Tower Marketplace — AWS Marketplace oferece uma ampla variedade de soluções para o AWS Control Tower para ajudar você a integrar software de terceiros. Essas soluções ajudam a resolver os principais casos de uso operacionais 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).

Notas de lançamento do AWS Control Tower

As seções a seguir mostram detalhes sobre os lançamentos do AWS Control Tower que exigem uma atualização para uma zona de pouso do AWS Control Tower, bem como os lançamentos que são incorporados 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 no Histórico do documento.

Janeiro de 2025 - presente

Desde janeiro de 2025, o AWS Control Tower lançou as seguintes atualizações:

Janeiro - dezembro de 2024

Em 2024, o AWS Control Tower lançou as seguintes atualizações:

- O AWS Control Tower cFct suporta GitHub e RCPs
- O AWS Control Tower adiciona controles preventivos com políticas declarativas
- O AWS Control Tower adiciona opções de plano de backup prescritivo
- O AWS Control Tower integra AWS Config controles

- O AWS Control Tower melhora o gerenciamento de ganchos e adiciona regiões de controle proativas
- AWS Control Tower lança políticas gerenciadas de controle de recursos
- Relatórios da AWS Control Tower alteram a política de controle
- Nova `ResetEnabledControl` API
- `GetControl`API de atualizações do catálogo de controle
- O AWS Control Tower suporta o AFT GitLab
- O AWS Control Tower está disponível na região AWS Ásia-Pacífico (Malásia)
- AWS Control Tower é compatível com até mil contas por UO
- AWS Control Tower adiciona a seleção de versão da zona de pouso
- API de controle descritivo disponível, acesso expandido a regiões e controles
- AWS Control Tower é compatível com AFT e CfCT em regiões opcionais
- AWS Control Tower adiciona a API `ListLandingZoneOperations`
- AWS Control Tower permite até 100 operações de controle simultâneas
- AWS Control Tower disponível na região da AWS Oeste do Canadá (Calgary)
- AWS Control Tower permite ajustes na cota de autoatendimento
- AWS Control Tower lança o Guia de referência de controles
- AWS Control Tower atualiza e renomeia dois controles proativos
- Controles obsoletos não estão mais disponíveis
- O AWS Control Tower oferece suporte à marcação de `EnabledControl` recursos em AWS CloudFormation
- O AWS Control Tower oferece suporte APIs para registro e configuração de UO com linhas de base

O AWS Control Tower cFct suporta GitHub e RCPs

9 de dezembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte à GitHub TM™ como uma opção para um sistema de controle de versão (VCS) de terceiros e fonte de configuração para personalizações do AWS

Control Tower (CFCT). Para obter mais informações, consulte Configurar GitHub como fonte de configuração.

O AWS Control Tower agora oferece suporte a políticas de controle de recursos (RCPs) para personalizações da AWS Control Tower (CFCT). Para obter mais informações, consulte Guia de personalização do CfCT.

O AWS Control Tower adiciona controles preventivos com políticas declarativas

1 de dezembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte a controles preventivos que são implementados por políticas declarativas da AWS Organizations. As políticas declarativas são aplicadas diretamente no nível do serviço. Essa abordagem garante que a configuração especificada seja aplicada, mesmo quando novos recursos são introduzidos pelo serviço. APIs Para obter mais informações, consulte Controles implementados com políticas declarativas.

O AWS Control Tower adiciona opções de plano de backup prescritivo

25 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte a AWS Backup planos prescritivos que permitem incorporar um fluxo de trabalho de backup e recuperação de dados diretamente na sua landing zone. O plano de backup inclui regras predefinidas, como dias de retenção, frequência de backup e a janela de tempo durante a qual o backup ocorre. Essas regras definem como fazer backup de seus AWS recursos em todas as suas contas de membros governadas. Quando você aplica um plano de backup na landing zone, o AWS Control Tower garante que o plano seja consistente para todas as contas dos membros e esteja alinhado às recomendações de melhores práticas do AWS Backup.

Para obter mais informações, consulte AWS Backup e AWS Control Tower.

O AWS Control Tower integra AWS Config controles

21 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower integrou AWS Config controles selecionados para que possam ser visualizados e gerenciados pela AWS Control Tower.

Para obter mais informações, consulte AWS Config Controles integrados disponíveis no AWS Control Tower

O AWS Control Tower melhora o gerenciamento de ganchos e adiciona regiões de controle proativas

20 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Com essa versão, você pode utilizar a capacidade total dos AWS CloudFormation ganchos, sem restrições do AWS Control Tower. Além disso, controles proativos estão disponíveis na região Oeste do Canadá (Calgary) e na região Ásia-Pacífico (Malásia).

Anteriormente, todos os AWS CloudFormation ganchos em seu ambiente precisavam ser protegidos pelo controle CT.CLOUDFORMATION.PR.1, para que somente o AWS Control Tower pudesse modificá-los. Com essa versão, você pode implantar AWS CloudFormation e modificar esses ganchos sem as restrições exigidas anteriormente pelo serviço AWS Control Tower.

Se você atualmente implanta controles proativos, pode migrar para essa funcionalidade aprimorada de gancho. Para redefinir todos os controles proativos em uma OU, redefina qualquer controle proativo único que esteja ativo nessa OU. Você pode realizar a redefinição chamando a `ResetEnabledControl` API ou atualizando o controle no console com a funcionalidade Redefinir. Quando você conclui essa tarefa de redefinição para qualquer controle proativo, o AWS Control Tower move todos os ganchos de controle proativo na OU para o novo recurso. Repita esse processo para cada UO que implanta controles proativos.

Depois de redefinir qualquer controle proativo, remova o controle CT.CLOUDFORMATION.PR.1 da sua AWS Control Tower OUs, a menos que você tenha habilitado esse controle para outra finalidade. Se você não desativar o controle CT.CLOUDFORMATION.PR.1, não poderá criar e modificar seus outros ganchos. AWS CloudFormation

Para obter mais informações, consulte Atualizar ganchos de controle proativos.

AWS Control Tower lança políticas gerenciadas de controle de recursos

15 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower oferece um novo tipo de controle preventivo, implementado com políticas de controle de recursos (RCPs). Esses controles ajudam você a estabelecer um perímetro de dados em todo o seu ambiente do AWS Control Tower, para proteger seus recursos contra acesso não intencional.

Por exemplo, você pode habilitar controles baseados em RCP para Amazon S3,,, AWS Security Token Service Amazon AWS Key Management Service SQS e serviços. AWS Secrets Manager Um controle baseado em RCP pode impor um requisito como “Exigir que os recursos do Amazon S3 da organização sejam acessíveis somente pelos diretores do IAM que pertencem à organização ou por um AWS serviço”, independentemente das permissões concedidas em políticas de bucket individuais.

Você pode configurar os novos controles baseados em RCP e certos controles preventivos baseados em SCP existentes para especificar isenções de AWS IAM para diretores e recursos. Se você não quiser que um principal ou um recurso seja governado pelo controle, você pode configurar uma isenção.

Ao combinar controles preventivos, proativos e de detetive no AWS Control Tower, você pode monitorar se seu AWS ambiente de várias contas é seguro e gerenciado de acordo com as melhores práticas, como o padrão AWS Foundational Security Best Practices.

Esses novos controles preventivos baseados em RCP estão disponíveis Regiões da AWS onde o AWS Control Tower está disponível. Para obter uma lista completa de Regiões da AWS onde o AWS Control Tower está disponível, consulte a Região da AWS tabela.

Relatórios da AWS Control Tower alteram a política de controle

15 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora relata desvios na política de controle, para controles implementados com políticas de controle de recursos (RCPs) e controles que fazem parte do padrão gerenciado pelo serviço Security Hub: AWS Control Tower. Esse tipo de desvio pode ser corrigido por meio da nova `ResetEnabledControl` API. Consulte mais informações em Types of governance drift.

Nova **`ResetEnabledControl`** API

14 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower anuncia uma nova API para ajudar você a gerenciar o desvio de controle de forma programática. Você pode reparar o desvio do controle e redefinir um controle para a configuração pretendida. A `ResetEnabledControl` API funciona com controles opcionais do AWS Control Tower, incluindo controles eletivos e altamente recomendados.

Exceções de controle

- Os controles implementados com políticas de controle de serviço (SCPs) não podem ser redefinidos com essa API. Para obter mais informações, consulte `ResetEnabledControl`.
- Os controles obrigatórios não podem ser redefinidos, pois eles protegem os recursos do AWS Control Tower.
- O controle de negação de região para o landing zone deve ser redefinido por meio do console.

O desvio de controle ocorre quando um controle da AWS Control Tower é modificado fora da AWS Control Tower, por exemplo, a partir do AWS Organizations console. Resolver desvios ajuda a garantir a conformidade com os requisitos de governança.

`GetControl`API de atualizações do catálogo de controle

8 de novembro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte a uma `GetControl` API atualizada que inclui dois novos campos: `Implementation` tipos para todos os controles e `Parameters` para determinados controles que podem ser configurados.

A `GetControl` API faz parte do `controlcatalog` namespace do AWS Control Tower.

Para obter mais informações, consulte a `GetControl`API na Referência da API do Control Catalog.

Essa versão inclui alterações relacionadas que são mostradas no console do AWS Control Tower.

- Todos os AWS Security Hub controles existentes têm seus valores de `Implementation` parâmetros alterados de AWS Config regra para AWS Security Hub. O painel de ajuda do console correspondente foi modificado para refletir essa alteração.

- Todos os controles Hook existentes têm seus valores de `Implementation` parâmetros alterados de regra de AWS CloudFormation guarda para AWS CloudFormation gancho. O painel de ajuda do console correspondente foi modificado para refletir essa alteração.

O AWS Control Tower suporta o AFT GitLab

23 de outubro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte à GitLab TM™ e ao GitLab autogerenciamento como opções para um sistema de controle de versão (VCS) de terceiros e fonte de configuração para o Account Factory for Terraform (AFT).

O AWS Control Tower está disponível na região AWS Ásia-Pacífico (Malásia)

21 de outubro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower está disponível na região da AWS Ásia-Pacífico (Malásia).

Consulte uma lista completa das regiões em que o AWS Control Tower está disponível na Tabela de regiões da AWS.

AWS Control Tower é compatível com até mil contas por UO

30 de agosto de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower aumentou o número máximo de contas permitidas por unidade organizacional (UO) de 300 para 1.000. Agora, você pode inscrever até 1.000 Contas da AWS na governança do AWS Control Tower de uma só vez, sem alterar sua estrutura de OU. Os processos de registro e novo registro da UO também estão mais eficientes, exigindo muito menos tempo para implantar os recursos da linha de base do AWS Control Tower em suas contas.

Algumas limitações da conta ainda se aplicam devido às limitações no número de conjuntos de pilhas do AWS CloudFormation disponíveis. Especificamente, o número máximo de contas que

você pode inscrever em uma UO pode variar, dependendo do número de regiões que tem sob governança. Para saber mais, acesse Limitações com base nos AWS serviços subjacentes no Guia do usuário do AWS Control Tower. Consulte uma lista completa de Regiões da AWS em que o AWS Control Tower está disponível na Tabela de regiões da Região da AWS.

AWS Control Tower adiciona a seleção de versão da zona de pouso

15 de agosto de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Se estiver executando a versão 3.1 ou posterior da zona de pouso do AWS Control Tower, você poderá atualizar ou reparar a zona de pouco no local na versão atual, ou poderá fazer upgrade para uma versão de sua escolha. Anteriormente, qualquer atualização ou reparo da zona de pouso exigia um upgrade para a versão mais recente dela.

Com a seleção de versão da zona de pouso, você tem mais flexibilidade para planejar atualizações de versão enquanto avalia possíveis mudanças no ambiente. Você não precisa escolher entre reparar o desvio para manter a conformidade, atualizar as configurações da zona de pouso ou atualizar para a versão mais recente da zona de pouso. Se estiver executando a versão 3.1 ou posta da zona de pouso, você poderá optar por permanecer na versão atual ou fazer upgrade para uma versão mais nova ao atualizar ou redefinir as configurações da zona de pouso.

API de controle descritivo disponível, acesso expandido a regiões e controles

6 de agosto de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower adicionou duas novas operações de API que ajudam a encontrar mais informações sobre os controles disponíveis de forma programática. Essa funcionalidade facilita a implantação de controles com automação.

- A API `GetControl` retorna detalhes sobre um controle habilitado, incluindo o identificador de destino, um resumo das informações de controle, uma lista de regiões de destino e o status do desvio.
- A API `ListControls` retorna uma lista paginada de todos os controles disponíveis na biblioteca de controles do AWS Control Tower.

Eles APIs são acessados por meio do namespace AWS Control Catalog. O Catálogo de AWS Controle faz parte do AWS Control Tower, que inclui controles que ajudam você a gerenciar outros AWS serviços, não apenas o AWS Control Tower. Esse catálogo expandido consolida controles de vários AWS serviços, para que você possa visualizar AWS os controles de acordo com alguns casos de uso comuns, como: segurança, custo, durabilidade e operações. Consulte mais informações na Referência da API do Control Catalog.

Disponibilidade expandida da região

A partir desse lançamento, você pode estender a governança do AWS Control Tower nas Regiões da AWS onde alguns dos seus controles (já) habilitados não estejam disponíveis. Além disso, agora é possível habilitar determinados controles em mais regiões, mesmo que o controle não seja compatível com todas as suas regiões administradas.

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 administradas. Com esse lançamento, você tem mais flexibilidade e responsabilidade de garantir que a configuração esteja correta para todos os controles habilitados e todas as regiões administradas. O controle do AWS Control Tower APIs e o catálogo de controle APIs podem ajudá-lo a obter informações sobre as AWS regiões nas quais você está protegido por controles habilitados e as regiões nas quais controles adicionais podem ser implantados. As informações de região e controle também estão disponíveis no console do AWS Control Tower.

AWS Control Tower é compatível com AFT e CfCT em regiões opcionais

18 de julho de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Atualmente, as estruturas de personalização da AWS Control Tower Account Factory for Terraform (AFT) e Customizations for AWS Control Tower (CFCt) estão disponíveis em mais cinco Regiões da AWS: Ásia-Pacífico (Hyderabad, Jacarta e Osaka), Israel (Tel Aviv) e Oriente Médio (Emirados Árabes Unidos).

O Account Factory for Terraform (AFT) configura um pipeline do Terraform para ajudar a provisionar e personalizar contas no AWS Control Tower. As personalizações do AWS Control Tower (cFct) ajudam você a personalizar sua zona de pouso e contas da AWS Control Tower com AWS CloudFormation modelos e políticas de controle de serviços (). SCPs

Para saber mais, acesse as páginas do Account Factory for Terraform e do Customizations for AWS Control Tower no Guia do usuário do AWS Control Tower. Você também pode consultar as notas de lançamento na página do AFT no Github e na página do CfCT no Github. AFT e cFct são suportados em todas as AWS regiões, com algumas exceções. Consulte detalhes em Region limitations.

AWS Control Tower adiciona a API `ListLandingZoneOperations`

26 de junho de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower adicionou uma API que permite recuperar uma lista das operações aplicadas recentemente à zona de pouso e das operações atualmente em andamento. A API pode retornar o histórico das operações da zona de pouso e seus identificadores por até 90 dias. Consulte exemplos de uso em View the status of your landing zone operations.

Consulte mais informações sobre a API `ListLandingZoneOperations` em `ListLandingZoneOperations` na Referência de API do AWS Control Tower.

AWS Control Tower permite até 100 operações de controle simultâneas

20 de maio de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora é compatível com várias operações de controle com maior simultaneidade. Você pode enviar até 100 operações de controle do AWS Control Tower, em várias unidades organizacionais (OUs), ao mesmo tempo, a partir do console ou com APIs. Até dez (10) operações podem ser executadas simultaneamente, e as adicionais são colocadas na fila. Dessa forma, você pode definir uma configuração mais padronizada em várias Contas da AWS, sem a carga operacional das operações de controle repetitivas.

Para monitorar o status das operações de controle em andamento e na fila, você pode acessar a nova página Operações recentes no console do AWS Control Tower ou pode chamar a nova API `ListControlOperations`.

A biblioteca do AWS Control Tower contém mais de 500 controles, que são mapeados para diferentes serviços, frameworks e objetivos de controle. Para um objetivo de controle específico, como Criptografar dados em repouso, é possível habilitar vários controles com uma única operação

de controle, para ajudar a atingir o objetivo. Esse recurso facilita o desenvolvimento acelerado, permite a adoção mais rápida dos controles de práticas recomendadas e reduz as complexidades operacionais.

AWS Control Tower disponível na região da AWS Oeste do Canadá (Calgary)

3 de maio de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

A partir de hoje, é possível ativar o AWS Control Tower na região Oeste do Canadá (Calgary). Se você já implantou o AWS Control Tower e deseja estender seus recursos de governança para essa região, você 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 as regiões e atualize a zona de pouso.

A região Oeste do Canadá (Calgary) não é compatível com o 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 Oeste do Canadá (Calgary) como a região de origem, os procedimentos para atualizar contas, configurar automações de contas e todos os outros processos que envolvam o Service Catalog serão diferentes dos de outras regiões.

Provisionar contas

Para criar e provisionar uma conta na região Oeste do Canadá (Calgary), recomendamos que você crie uma conta fora do AWS Control Tower e, depois, inscreva-a em uma UO registrada. Consulte mais informações em Enroll an existing account e em Steps to enroll an account.

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.

O Account Factory Customization (AFC), o Account Factory for Terraform (AFT) e o Customizations for AWS Control Tower (CfCT) não estão disponíveis na região Oeste do Canadá (Calgary), devido à falta de outras dependências subjacentes do AWS Control Tower. Se estender a governança para a região Oeste do Canadá (Calgary), você poderá continuar gerenciando os esquemas do AFC em todas as regiões compatíveis com o AWS Control Tower, desde que o Service Catalog esteja disponível na região de origem.

Controles

Controles e controles proativos para o Padrão gerenciado por serviços do AWS Security Hub : AWS Control Tower não estão disponíveis na região Oeste do Canadá (Calgary). O controle preventivo `CT.CLOUDFORMATION.PR.1` não está disponível na região Oeste do Canadá (Calgary) porque ele é necessário apenas para ativar os controles proativos baseados em hook. Certos controles de detetive baseados em não AWS Config estão disponíveis. Para obter detalhes, consulte Limitações de controle.

Provedor de identidades

O Centro de Identidade do IAM não está disponível na região Oeste do Canadá (Calgary). As práticas recomendadas instruem a configurar a zona de pouso em uma região onde o Centro de Identidade do IAM esteja disponível. Como alternativa, você tem a opção de autogerenciar a configuração de acesso à conta se usar um provedor de identidades externo na região Oeste do Canadá (Calgary).

A indisponibilidade do Service Catalog na região Oeste do Canadá (Calgary) não afeta outras regiões compatíveis com o AWS Control Tower. Essas diferenças serão aplicadas somente se a região de origem for Oeste do Canadá (Calgary).

Consulte uma lista completa das regiões em que o AWS Control Tower está disponível na Tabela de regiões da AWS.

AWS Control Tower permite ajustes na cota de autoatendimento

25 de abril de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora permite ajustes na cota de autoatendimento por meio do console Service Quotas. Para obter mais informações, consulte Solicitar um aumento da cota.

AWS Control Tower lança o Guia de referência de controles

21 de abril de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower lançou o Guia de referência de controles, um novo documento no qual você pode encontrar informações detalhadas sobre os controles específicos do ambiente do 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. Consulte mais informações no Guia de referência de controles do AWS Control Tower.

AWS Control Tower atualiza e renomeia dois controles proativos

26 de março de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS 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 versão mínima do TLS do domínio do serviço. Para fazer essa atualização no ambiente, é necessário Desabilitar e Habilitar 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.

Se tiver dúvidas ou solicitações, entre em contato com o AWS Support.

Controles obsoletos não estão mais disponíveis

12 de março de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower desativou alguns controles. Esses controles não estarão 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

O AWS Control Tower oferece suporte à marcação de **`EnabledControl`** recursos em AWS CloudFormation

22 de fevereiro de 2024

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Esse lançamento do AWS Control Tower atualiza o comportamento do recurso `EnabledControl`, para se alinhar melhor aos controles configuráveis e melhorar a capacidade de gerenciar o ambiente do AWS Control Tower com automação. Com esse lançamento, é possível adicionar tags a recursos `EnabledControl` configuráveis por meio de modelos do AWS CloudFormation . Anteriormente, você podia adicionar tags APIs somente por meio do console do AWS Control Tower.

As operações de API `GetEnabledControl`, `EnableControl` e `ListTagsforResource` do AWS Control Tower são atualizadas com esse lançamento, pois dependem da funcionalidade do recurso `EnabledControl`.

Consulte mais informações em Tagging `EnabledControl` resources in AWS Control Tower e em `EnabledControl` no Guia do usuário do AWS CloudFormation .

O AWS Control Tower oferece suporte APIs para registro e configuração de UO com linhas de base

14 de fevereiro de 2024

(Não é necessário atualizar a zona de pouso do 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 UO, as contas-membros dentro da UO são inscritas na governança do AWS Control Tower. Algumas ressalvas podem se aplicar. Por exemplo, o registro de UO por meio do console do AWS Control Tower habilita controles opcionais, bem como controles obrigatórios. Ao ligar APIs, talvez seja necessário concluir uma etapa extra para que os controles opcionais sejam ativados.

Uma linha de base do AWS Control Tower incorpora as práticas recomendadas para a governança do AWS Control Tower de uma UO e contas-membros. Por exemplo, quando você habilita uma linha de base em uma OU, as contas membros dentro da OU recebem um grupo definido de recursos, incluindo, AWS CloudTrail AWS Config, IAM Identity Center e as funções necessárias AWS do IAM.

As linhas de base específicas são compatíveis com versões específicas da zona de pouso do AWS Control Tower. O AWS Control Tower pode aplicar a linha de base compatível mais recente à zona de pouso quando você altera as configurações de zona inicial. Para obter mais informações, consulte Compatibilidade das linhas de base da UO e das versões da zona de pouso.

Esse lançamento inclui quatro Tipos de linhas de base essenciais

- `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 do 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 do AWS Control Tower.

Para saber mais sobre elas APIs, analise as linhas de base no Guia do usuário do AWS Control Tower e na referência da API. Os novos APIs estão disponíveis Regiões da AWS onde o AWS Control Tower está disponível, exceto nas regiões GovCloud (EUA). Para obter uma lista de Regiões da AWS onde o AWS Control Tower está disponível, consulte a Região da AWS tabela.

De janeiro a dezembro de 2023

Em 2023, o AWS Control Tower lançou as seguintes atualizações:

- Transição para um novo tipo de produto AWS Service Catalog externo (fase 3)
- Versão 3.3 da zona de pouso do AWS Control Tower
- Transição para um novo tipo de produto AWS Service Catalog externo (fase 2)
- AWS Control Tower anuncia controles para auxiliar a soberania digital
- O AWS Control Tower é compatível com landing zone APIs
- AWS Control Tower permite a marcação de controles habilitados
- AWS Control Tower disponível na região Ásia-Pacífico (Melbourne)
- Transição para um novo tipo de produto AWS Service Catalog externo (fase 1)
- Nova API de controle disponível
- AWS Control Tower adiciona outros controles
- Novo tipo de desvio relatado: acesso confiável desabilitado
- Quatro adicionais Regiões da AWS
- AWS Control Tower disponível na região Tel Aviv
- AWS Control Tower lança 28 novos controles proativos
- AWS Control Tower desativa dois controles
- Versão 3.2 da zona de pouso do AWS Control Tower
- AWS Control Tower gerencia contas com base em ID

- Controles de detecção adicionais do Security Hub disponíveis na biblioteca de controles do AWS Control Tower
- AWS Control Tower publica tabelas de metadados de controle
- Suporte do Terraform para o Account Factory Customization
- AWS Autogerenciamento do IAM Identity Center disponível para landing zone
- O AWS Control Tower aborda a governança mista para OUs
- Controles proativos adicionais disponíveis
- Controles EC2 proativos atualizados da Amazon
- Sete adicionais Regiões da AWS disponíveis
- Rastreamento de solicitações de personalização de conta do Account Factory for Terraform (AFT)
- Versão 3.1 da zona de pouso do AWS Control Tower
- Controles proativos disponíveis ao público

Transição para um novo tipo de produto AWS Service Catalog externo (fase 3)

14 de dezembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS 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 tipo de produto AWS Service Catalog externo.

Se não atualizar os esquemas da conta para usar o tipo de produto External, você só poderá atualizar ou encerrar contas que provisionou usando esquemas do Terraform Open Source.

Versão 3.3 da zona de pouso do AWS Control Tower

14 de dezembro de 2023

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 3.3. Consulte informações em Atualizar a zona de pouso).

Atualizações na política de bucket do S3 na conta de auditoria do AWS Control Tower

Modificamos a política de bucket de auditoria do Amazon S3 que o AWS Control Tower implanta nas contas, de modo que uma condição `aws:SourceOrgID` deve ser atendida para qualquer permissão de gravação. Com essa versão, AWS os serviços têm acesso aos seus recursos somente quando a solicitação é originada da sua organização ou unidade organizacional (OU).

É possível usar a chave de condição `aws:SourceOrgID` e definir o valor do ID da organização no elemento de condição da 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 S3 do AWS Control Tower.

Fizemos essa alteração para corrigir uma possível vulnerabilidade de segurança, sem afetar a funcionalidade das workloads existentes. Consulte a política atualizada em Política de bucket do Amazon S3 na conta de auditoria.

Para obter mais informações sobre a nova 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”.

Atualizações da política no tópico do AWS Config SNS

Adicionamos a nova chave de `aws:SourceOrgID` condição à política do tópico AWS Config SNS. Para ver a política atualizada, consulte A política de tópicos do AWS Config SNS.

Atualizações no controle de negação de região da zona de pouso

- `discovery-marketplace:` removido. Essa ação é coberta pela isenção `aws-marketplace:*`.
- `quicksight:DescribeAccountSubscription` adicionado

AWS CloudFormation Modelo atualizado

Atualizamos o AWS CloudFormation modelo da pilha chamada para `BASELINE-CLOUDTRAIL-MASTER` que ela não mostre desvio quando a AWS KMS criptografia não for usada.

Transição para um novo tipo de produto AWS Service Catalog externo (fase 2)

7 de dezembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

HashiCorp atualizou seu licenciamento do Terraform. Como resultado, AWS Service Catalog alterou o suporte para produtos Terraform Open Source e provisionou produtos para um novo tipo de produto, chamado Externo.

Para evitar interrupções nas cargas de trabalho e nos AWS recursos existentes em suas contas, siga as etapas de transição do AWS Control Tower em Transição para o tipo de produto AWS Service Catalog externo até 14 de dezembro de 2023.

AWS Control Tower anuncia controles para auxiliar a soberania digital

27 de novembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower anuncia 65 novos controles AWS gerenciados para ajudar você a atender aos seus requisitos de soberania digital. Com esse lançamento, é possível descobrir esses controles sob um novo grupo de soberania digital no console do AWS Control Tower. É possível 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. Consulte mais informações sobre controles de soberania digital em Controls that enhance digital sovereignty protection.

Por exemplo, você pode optar por ativar controles que ajudem a aplicar suas estratégias de criptografia e resiliência, como Exigir um cache de AWS AppSync API para ter a criptografia em trânsito ativada ou Exigir que um Firewall de AWS Rede seja implantado em várias zonas de disponibilidade. Você também pode personalizar o controle de negação de região do AWS Control Tower para aplicar restrições regionais que melhor atendam às suas necessidades comerciais exclusivas.

Esse lançamento traz recursos bem aprimorados de negação de região do AWS Control Tower. É possível aplicar um novo controle de negação de região parametrizado no nível da UO, para aumentar a granularidade da governança e, ao mesmo tempo, manter a governança adicional da região no nível da zona de pouso. Esse controle de negação de região personalizável ajuda você a aplicar restrições regionais que melhor atendam às suas necessidades comerciais exclusivas. Consulte mais informações sobre o novo controle de negação de região configurável em Region deny control applied to the OU.

Como uma nova ferramenta para o novo aprimoramento de negação de região, esse lançamento inclui uma nova API `UpdateEnabledControl`, que permite redefinir os controles habilitados para

as configurações padrão. Essa API é especialmente útil em casos de uso em que você precisa resolver o desvio rapidamente ou para garantir de forma programática que um controle não esteja em um estado de desvio. Consulte mais informações sobre a nova API na Referência de API do AWS Control Tower.

Novos controles proativos

- CT.APIGATEWAY.PR.6: Exija um domínio REST do Amazon API Gateway para usar uma política de segurança que especifique uma versão mínima do protocolo TLS de .2 TLSv1
- CT.APPSYNC.PR.2: Exigir que uma API AWS AppSync GraphQL seja configurada com visibilidade privada
- CT.APPSYNC.PR.3: Exija que uma API AWS AppSync GraphQL não seja autenticada com chaves de API
- CT.APPSYNC.PR.4: Exigir um cache da API AWS AppSync GraphQL para ter a criptografia em trânsito ativada.
- CT.APPSYNC.PR.5: Exigir um cache da API AWS AppSync GraphQL para ter a criptografia em repouso ativada.
- CT.AUTOSCALING.PR.9: Exija um volume do Amazon EBS 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 tipos de instância AWS Nitro ao substituir um modelo de execução
- CT.AUTOSCALING.PR.11: Exija que somente os tipos de instância AWS Nitro que suportem criptografia de tráfego de rede entre instâncias sejam adicionados a um grupo do Amazon EC2 Auto Scaling, ao substituir um modelo de execução
- CT.DAX.PR.3: exija um cluster do DynamoDB Accelerator para criptografar dados em trânsito com o Transport Layer Security (TLS).
- CT.DMS.PR.2: Exigir um endpoint do AWS Database Migration Service (DMS) para criptografar conexões para endpoints de origem e destino
- CT.EC2.PR.15: Exija que uma EC2 instância da Amazon use um tipo de instância AWS Nitro ao criar a partir do tipo de `AWS::EC2::LaunchTemplate` recurso
- CT.EC2.PR.16: Exija que uma EC2 instância da Amazon use um tipo de instância AWS Nitro quando criada usando o tipo `AWS::EC2::Instance` de recurso
- CT.EC2.PR.17: Exigir um host EC2 dedicado da Amazon para usar um tipo de instância do AWS Nitro

- CT.EC2.PR.18: Exija que uma EC2 frota da Amazon substitua somente os modelos de lançamento pelos tipos de instância AWS 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 pelos tipos de instância AWS Nitro que ofereçam 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 a autenticação RBAC ativada
- CT.MQ.PR.1: exija que um agente do Amazon MQ ActiveMQ use o modo de implantação ativo/em espera para alta disponibilidade.
- CT.MQ.PR.2: exija que um agente do Amazon MQ Rabbit MQ use o modo de cluster multi-AZ para alta disponibilidade.
- CT.MSK.PR.1: exija um cluster do Amazon Managed Streaming for Apache Kafka (MSK) para aplicar a criptografia em trânsito entre os nós do agente de cluster.
- CT.MSK.PR.2: Exija que um cluster Amazon Managed Streaming for Apache Kafka (MSK) seja configurado com desativado PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Exigir que um firewall de Firewall de AWS Rede seja implantado em várias zonas de disponibilidade
- CT.RDS.PR.26: exija um proxy de banco de dados do Amazon RDS para requerer conexões de Transport Layer Security (TLS).
- CT.RDS.PR.27: exija um grupo de parâmetros de cluster de banco de dados do Amazon RDS para requerer conexões de Transport Layer Security (TLS) para tipos de mecanismos compatíveis.
- CT.RDS.PR.28: exija um grupo de parâmetros de banco de dados do Amazon RDS para requerer conexões de Transport Layer Security (TLS) para tipos de mecanismos compatíveis.
- CT.RDS.PR.29: Exija que um cluster Amazon RDS não esteja configurado para ser acessível publicamente por meio da propriedade 'PubliclyAccessible'
- CT.RDS.PR.30: exija que uma instância de banco de dados do Amazon RDS tenha a criptografia em repouso configurada para usar uma chave do KMS que você especifique para os tipos de mecanismos compatíveis.
- CT.S3.PR.12: exija que um ponto de acesso Amazon S3 tenha uma configuração de Bloqueio de Acesso Público (BPA) com todas as opções definidas como verdadeiras.

Novos controles preventivos

- CT.APPSYNC.PV.1 Exija que uma API AWS AppSync GraphQL esteja configurada com visibilidade privada
- CT.EC2.PV.1 Exija que um snapshot do Amazon EBS seja criado a partir de um volume criptografado EC2
- CT.EC2.PV.2 Exija que um volume anexado do Amazon EBS esteja configurado para criptografar dados em repouso
- CT.EC2.PV.3 Exija que um snapshot do Amazon EBS não possa ser restaurado publicamente
- CT.EC2.PV.4 Exija que o Amazon EBS direct não APIs 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 ações obsoletas da Amazon e da API EC2 RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1 Exija que uma política AWS KMS fundamental tenha uma declaração que limite a criação de AWS KMS subsídios a AWS serviços
- CT.KMS.PV.2 Exija que uma chave AWS KMS assimétrica com material de chave RSA usado para criptografia não tenha um comprimento de chave de 2048 bits
- CT.KMS.PV.3 Exija que uma AWS KMS chave seja configurada com a verificação de segurança de bloqueio de política de desvio ativada
- CT.KMS.PV.4 Exija que uma chave AWS KMS gerenciada pelo cliente (CMK) seja configurada com material de chave proveniente do CloudHSM AWS
- CT.KMS.PV.5 Exigir que uma chave AWS KMS gerenciada pelo cliente (CMK) seja configurada com material de chave importado
- CT.KMS.PV.6 Exija que uma chave AWS KMS gerenciada pelo cliente (CMK) seja configurada com material de chaves proveniente de um armazenamento de chaves externo (XKS)
- CT.LAMBDA.PV.1 Exigir um URL de AWS Lambda função para usar a autenticação AWS baseada em IAM
- CT.LAMBDA.PV.2 Exija que um URL de AWS Lambda função seja configurado para acesso somente por diretores dentro de seu Conta da AWS
- CT.MULTISERVICE.PV.1: Negar acesso AWS com base na solicitação de uma unidade organizacional Região da AWS

Os novos controles de detetives que aprimoram sua postura de governança de soberania digital fazem parte do AWS Control Tower padrão gerenciado AWS Security Hub por serviços.

Novos controles de detecção

- SH.ACM.2: os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- SH.AppSync.5: O AWS AppSync GraphQL não APIs deve ser autenticado com chaves de 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 endpoints do DMS 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 anexos de VPC
- SH.EKS.1: os endpoints do cluster do EKS 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 AUTH ativado
- SH.EventBridge.3: os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- SH.KMS.4: a rotação de AWS KMS chaves deve estar ativada
- SH.Lambda.3: as funções do Lambda devem estar em uma VPC.
- SH.MQ.5: os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera.
- SH.MQ.6: os agentes do RabbitMQ devem usar o modo de implantação de cluster.
- SH.MSK.1: os clusters do MSK devem ser criptografados em trânsito entre os nós do agente.

- SH.RDS.12: a autenticação do IAM deve ser configurada para clusters do RDS.
- SH.RDS.15: os clusters de banco de dados do RDS devem ser configurados com várias zonas de disponibilidade.
- SH.S3.17: os buckets S3 devem ser criptografados em repouso com chaves AWS KMS

Para obter mais informações sobre controles adicionados ao padrão AWS Security Hub gerenciado por serviços (AWS Control Tower), consulte Controles que se aplicam ao Service-Managed Standard: AWS Control Tower na documentação. AWS Security Hub

Para obter uma lista dos Regiões da AWS que não oferecem suporte a determinados controles que fazem parte do AWS Control Tower padrão AWS Security Hub gerenciado por serviços, consulte Regiões sem suporte.

Novo controle configurável de negação de região no nível da UO

CT.MULTISERVICE.PV.1: esse controle aceita parâmetros para especificar regiões isentas, entidades principais do IAM e ações que são permitidas, no nível da UO, em vez de para toda a zona de pouso do AWS Control Tower. É um controle preventivo, implementado pela política de controle de serviços (SCP).

Consulte mais informações em Region deny control applied to the OU.

A API do **`UpdateEnabledControl`**

Esse lançamento do AWS Control Tower adiciona o seguinte suporte de API para controles:

- A API `EnableControl` atualizada pode configurar controles que são configuráveis.
- A API `GetEnabledControl` atualizada mostra os parâmetros configurados em um controle habilitado.
- A nova API `UpdateEnabledControl` pode alterar os parâmetros em um controle habilitado.

Consulte mais informações na Referência de API do AWS Control Tower.

O AWS Control Tower é compatível com landing zone APIs

26 de novembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora suporta a configuração e o lançamento da landing zone usando APIs. Você pode criar, atualizar, obter, listar, redefinir e excluir zonas de pouso usando APIs.

O seguinte APIs permite que você configure e gerencie sua landing zone programaticamente usando AWS CloudFormation ou o. AWS CLI

O AWS Control Tower oferece suporte ao seguinte APIs para zonas de pouso:

- `CreateLandingZone`: essa chamada de API cria uma zona de pouso usando uma versão da zona de pouso e um arquivo de manifesto.
- `GetLandingZoneOperation`: essa chamada de API retorna o status de uma operação de zona de pouso especificada.
- `GetLandingZone`: essa chamada de API retorna detalhes sobre a zona de pouso especificada, incluindo a versão, o arquivo de manifesto e o status.
- `UpdateLandingZone`: essa chamada de API atualiza a versão da zona de pouso ou o arquivo de manifesto.
- `ListLandingZone`: essa chamada de API retorna um identificador da zona de pouso (ARN) para uma configuração da zona de pouso na conta de gerenciamento.
- `ResetLandingZone`: essa chamada de API redefine a zona de pouso para os parâmetros especificados na atualização mais recente, o que pode reparar o desvio. Se a zona de pouso não tiver sido atualizada, essa chamada a redefinirá para os parâmetros especificados na criação.
- `DeleteLandingZone`: essa chamada de API desativa a zona de pouso.

Para começar com o landing zone APIs, veja Comece a usar o AWS Control Tower usando APIs o.

AWS Control Tower permite a marcação de controles habilitados

10 de novembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte à marcação de recursos para controles habilitados, a partir do console do AWS Control Tower ou por meio de APIs. É possível adicionar, remover ou listar tags para controles habilitados.

Com o lançamento do seguinte APIs, você pode configurar tags para os controles que você habilita 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.

O AWS Control Tower oferece suporte ao seguinte APIs para marcação de controle:

- `TagResource`: essa chamada de API adiciona tags aos controles habilitados no AWS Control Tower.
- `UntagResource`: essa chamada de API remove as tags dos controles habilitados no AWS Control Tower.
- `ListTagsForResource`: essa chamada de API retorna tags para controles habilitados no AWS Control Tower.

Os controles da AWS Control Tower APIs estão disponíveis Regiões da AWS onde a AWS Control Tower está disponível. Para obter uma lista completa dos locais Regiões da AWS em que o AWS Control Tower está disponível, consulte a tabela de AWS regiões. Para obter uma lista completa do AWS Control Tower APIs, consulte a Referência da API.

AWS Control Tower disponível na região Ásia-Pacífico (Melbourne)

3 de novembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower está disponível na região Ásia-Pacífico (Melbourne).

Se você já usa o AWS Control Tower e deseja estender seus recursos de governança para essa região em suas contas, acesse a página Configurações no painel do AWS Control Tower, selecione a região e atualize a zona de pouso. Depois de atualizar a landing zone, você deve atualizar todas as contas que são governadas pelo AWS Control Tower para colocar suas contas OUs sob governança na nova região. Consulte mais informações em About Updates.

Consulte uma lista de regiões nas quais o AWS Control Tower está disponível na Tabela de Região da AWS.

Transição para um novo tipo de produto AWS Service Catalog externo (fase 1)

31 de outubro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

HashiCorp atualizou seu licenciamento do Terraform. Como resultado, AWS Service Catalog atualizou o suporte para produtos Terraform Open Source e provisionou produtos para um novo tipo de produto, chamado Externo.

O AWS Control Tower não permite personalizações do Account Factory que dependem do tipo de produto External do AWS Service Catalog . Para evitar interrupções nas cargas de trabalho e nos AWS recursos existentes em suas contas, siga as etapas de transição do AWS Control Tower nesta ordem sugerida, até 14 de dezembro de 2023:

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. Acesse AWS Service Catalog e duplique todos os blueprints existentes do Terraform Open Source para usar o novo tipo de produto externo. Não encerre os esquemas existentes do Terraform Open Source.
3. Continue usando os esquemas existentes do Terraform Open Source para criar ou atualizar contas no AWS Control Tower.

Nova API de controle disponível

14 de outubro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora é compatível com uma API adicional que você pode usar para implantar e gerenciar controles do AWS Control Tower em grande escala. Para obter mais informações sobre o controle do AWS Control Tower APIs, consulte a Referência da API.

O AWS Control Tower adicionou uma nova API de controle.

- `GetEnabledControl`: a chamada de API fornece detalhes sobre um controle habilitado.

Também atualizamos esta API:

`ListEnabledControls`: essa chamada de API lista os controles habilitados pelo AWS Control Tower na unidade organizacional especificada e as contas que ela contém. Agora, ela retorna informações adicionais em um objeto `EnabledControlSummary`.

Com eles APIs, você pode realizar várias operações comuns de forma programática. Por exemplo:

- Consulte uma lista de todos os controles que você habilitou na biblioteca de controles do AWS Control Tower.
- Para qualquer controle habilitado, é possível ter informações sobre as regiões compatíveis com o controle, além do identificador (ARN), do status de desvio e do resumo do status do controle.

Os controles da AWS Control Tower APIs estão disponíveis Regiões da AWS onde a AWS Control Tower está disponível. Para obter uma lista completa dos locais Regiões da AWS em que o AWS Control Tower está disponível, consulte a tabela de AWS regiões. Para obter uma lista completa do AWS Control Tower APIs, consulte a Referência da API.

AWS Control Tower adiciona outros controles

5 de outubro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower anuncia novos controles proativos e de detecção.

Os controles proativos no AWS Control Tower são implementados por meio de AWS CloudFormation Hooks, que identificam e bloqueiam recursos não compatíveis antes de provisioná-los. AWS CloudFormation Os controles proativos complementam os recursos existentes de controle preventivo e de detecção 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 uma chave (KMS) AWS Key Management Service
- [CT.CLOUDTRAIL.PR.4] Exigir um armazenamento de dados de eventos do AWS CloudTrail Lake para habilitar a criptografia em repouso com uma AWS KMS chave
- [CT.DAX.PR.2] Exigir um cluster Amazon DAX para implantar nós em pelo menos três zonas de disponibilidade
- [CT.EC2.PR.14] Exigir um volume do Amazon EBS configurado por meio de um modelo de EC2 lançamento da Amazon para criptografar dados em repouso

- [CT.EKS.PR.2] Exigir que um cluster Amazon EKS seja configurado com criptografia secreta usando AWS chaves do Key Management Service (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 do Amazon EMR (EMR) esteja configurada para criptografar dados em repouso no Amazon S3
- [CT.EMR.PR.2] Exija que uma configuração de segurança do Amazon EMR (EMR) esteja configurada para criptografar dados em repouso no Amazon S3 com uma chave AWS KMS
- [CT.EMR.PR.3] Exija que uma configuração de segurança do Amazon EMR (EMR) seja configurada com criptografia de disco local de volume do EBS usando uma chave AWS KMS
- [CT.EMR.PR.4] Exija que uma configuração de segurança do Amazon EMR (EMR) esteja configurada para criptografar dados em trânsito
- [CT.GLUE.PR.1] Exigir que uma tarefa AWS Glue tenha uma configuração de segurança associada
- [CT.GLUE.PR.2] Exija uma configuração de segurança do AWS Glue para criptografar dados em destinos do Amazon S3 usando chaves KMS AWS
- [CT.KMS.PR.2] Exigir que uma chave AWS KMS assimétrica com material de chave RSA usado para criptografia tenha um comprimento de chave maior que 2048 bits
- [CT.KMS.PR.3] Exigir que uma política AWS KMS fundamental tenha uma declaração que limite a criação de AWS KMS subsídios a AWS serviços
- [CT.LAMBDA.PR.4] Exigir uma permissão de AWS Lambda camada para conceder acesso a uma AWS organização ou AWS conta específica
- [CT.LAMBDA.PR.5] Exigir um URL de AWS Lambda função para usar a autenticação AWS baseada em IAM
- [CT.LAMBDA.PR.6] Exigir uma política de URL CORS de AWS Lambda função para restringir o acesso a origens específicas
- [CT.NEPTUNE.PR.4] Exigir 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 comercialmente Regiões da AWS onde o AWS Control Tower está disponível. Consulte mais detalhes sobre esses controles em Proactive controls. Consulte mais detalhes sobre onde os controles estão disponíveis em Control limitations.

Novos controles de detecção

Novos controles foram adicionados ao padrão gerenciado por serviços do Security Hub: AWS Control Tower. Esses controles ajudam a aprimorar o procedimento de governança. Eles agem como parte do padrão gerenciado por serviços do Security Hub: AWS Control Tower, depois que você os habilita em qualquer UO 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 a autenticação de banco de dados do IAM habilitada
- [SH.Neptune.8] Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [SH.RDS.27] Os clusters de banco de dados do RDS devem ser criptografados em repouso

Os novos controles de AWS Security Hub detetive estão disponíveis na maioria dos Regiões da AWS lugares onde o AWS Control Tower está disponível. Consulte mais detalhes sobre esses controles em Controls that apply to Service-Managed Standard: AWS Control Tower. Consulte mais detalhes sobre onde os controles estão disponíveis em Limitações de controle.

Novo tipo de desvio relatado: acesso confiável desabilitado

21 de setembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Depois de configurar a zona de pouso do AWS Control Tower, é possível desabilitar o acesso confiável ao AWS Control Tower no AWS Organizations. No entanto, isso causa um desvio.

Com o tipo de desvio de acesso confiável desabilitado, o AWS Control Tower notifica você quando esse tipo de desvio ocorre, para que seja possível reparar a zona de pouso do AWS Control Tower. Consulte mais informações em Types of governance drift.

Quatro adicionais Regiões da AWS

13 de setembro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower já está disponível nas regiões Ásia-Pacífico (Hyderabad), Europa (Espanha e Zurique) e Oriente Médio (EAU).

Se você já usa o AWS Control Tower e deseja estender seus recursos de governança para essa região em suas contas, acesse a página Configurações no painel do AWS Control Tower, selecione a região e atualize a zona de pouso. Depois de atualizar a landing zone, você deve atualizar todas as contas que são governadas pelo AWS Control Tower para colocar suas contas OUs sob governança na nova região. Consulte mais informações em About Updates.

Consulte uma lista de regiões nas quais o AWS Control Tower está disponível na Tabela de Região da AWS.

AWS Control Tower disponível na região Tel Aviv

28 de agosto de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower anuncia disponibilidade na região Israel (Tel Aviv).

Se você já usa o AWS Control Tower e deseja estender seus recursos de governança para essa região em suas contas, acesse a página Configurações no painel do AWS Control Tower, selecione a região e atualize a zona de pouso. Depois de atualizar a landing zone, você deve atualizar todas as

contas que são governadas pelo AWS Control Tower para colocar suas contas OUs sob governança na nova região. Consulte mais informações em About Updates.

Consulte uma lista de regiões nas quais o AWS Control Tower está disponível na Tabela de Região da AWS.

AWS Control Tower lança 28 novos controles proativos

24 de julho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower está adicionando 28 novos controles proativos para ajudar a gerenciar o ambiente da AWS .

Os controles proativos aprimoram os recursos de governança do AWS Control Tower em seus AWS ambientes de várias contas, bloqueando recursos não compatíveis antes de serem provisionados. Esses controles ajudam a gerenciar AWS serviços como Amazon CloudWatch, Amazon Neptune, Amazon e ElastiCache AWS Step Functions 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 que uma AWS AppSync API GraphQL tenha o registro ativado
- [CT.CLOUDWATCH.PR.1] Exija que um alarme da CloudWatch Amazon tenha uma ação configurada para o estado do alarme
- [CT.CLOUDWATCH.PR.2] Exija que um grupo de registros da CloudWatch Amazon seja mantido por pelo menos um ano
- [CT.CLOUDWATCH.PR.3] Exija que um grupo de registros da CloudWatch Amazon seja criptografado em repouso com uma chave KMS AWS
- [CT.CLOUDWATCH.PR.4] Exigir que uma ação de alarme da Amazon seja ativada CloudWatch
- [CT.DOCUMENTDB.PR.1]: exija que um cluster Amazon DocumentDB seja criptografado em repouso.
- [CT.DOCUMENTDB.PR.2]: exija que um cluster do Amazon DocumentDB tenha backups automáticos habilitados.
- [CT.DYNAMODB.PR.2] Exija que uma tabela do Amazon DynamoDB seja criptografada em repouso usando chaves AWS KMS

- [CT. EC2.PR.13] Exija que uma EC2 instância da Amazon tenha o monitoramento detalhado ativado
- [CT.EKS.PR.1]: exija que um cluster do Amazon EKS seja configurado com o acesso público desabilitado ao endpoint do servidor da API do Kubernetes do cluster.
- [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 ElastiCache Amazon for Redis tenha as atualizações automáticas de versões secundárias ativadas
- [CT.ELASTICACHE.PR.3] Exija que um grupo de replicação ElastiCache Amazon for Redis tenha o failover automático ativado
- [CT.ELASTICACHE.PR.4] Exija que um grupo de replicação da Amazon tenha a criptografia em repouso ElastiCache ativada
- [CT.ELASTICACHE.PR.5] Exija que um grupo de replicação ElastiCache Amazon for Redis tenha a criptografia em trânsito ativada
- [CT.ELASTICACHE.PR.6] Exigir um cluster de cache da Amazon para usar um grupo de sub-rede personalizado ElastiCache
- [CT.ELASTICACHE.PR.7] Exija que um grupo de replicação da ElastiCache Amazon de versões anteriores do Redis tenha a autenticação do Redis AUTH
- [CT.ELASTICBEANSTALK.PR.3]: exija que um ambiente do AWS Elastic Beanstalk tenha uma configuração de registro em log.
- [CT.LAMBDA.PR.3]: exija que uma função do AWS Lambda esteja em uma Amazon Virtual Private Cloud (VPC) gerenciada pelo cliente.
- [CT.NEPTUNE.PR.1] Exija que um cluster de banco de dados Amazon Neptune tenha autenticação de banco de dados (IAM) AWS Identity and Access Management
- [CT.NEPTUNE.PR.2]: exija que um cluster de banco de dados do Amazon Neptune tenha a proteção contra exclusão habilitada.
- [CT.NEPTUNE.PR.3]: exija que um cluster de banco de dados do Amazon Neptune tenha a criptografia de armazenamento habilitada.
- [CT.REDSHIFT.PR.8]: exija que um cluster do Amazon Redshift seja criptografado.
- [CT.S3.PR.9]: exija que um bucket do Amazon S3 tenha o Bloqueio de Objetos do S3 ativado.
- [CT.S3.PR.10] Exija que um bucket Amazon S3 tenha a criptografia do lado do servidor configurada usando chaves AWS KMS

- [CT.S3.PR.11]: exija que um bucket do Amazon S3 tenha o versionamento habilitado.
- [CT.STEPFUNCTIONS.PR.1]: exija que uma máquina de estado do AWS Step Functions tenha o registro em log ativado.
- [CT.STEPFUNCTIONS.PR.2] Exigir que uma máquina de estado tenha o rastreamento ativado AWS Step Functions AWS X-Ray

Os controles proativos no AWS Control Tower são implementados por meio de AWS CloudFormation Hooks, que identificam e bloqueiam recursos não compatíveis antes de provisioná-los. AWS CloudFormation Os controles proativos complementam os recursos existentes de controle preventivo e de detecção no AWS Control Tower.

Esses novos controles proativos estão disponíveis em todos os Regiões da AWS lugares onde o AWS Control Tower está disponível. Consulte mais detalhes sobre esses controles em Proactive controls.

AWS Control Tower desativa dois controles

18 de julho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower conduz análises regulares de seus controles de segurança para garantir que eles estejam atualizados e continuem sendo considerados como práticas recomendadas. Os dois controles a seguir foram desativados, a partir de 18 de julho de 2023, e serão removidos da biblioteca de controles a partir de 18 de agosto de 2023. Não é mais possível habilitar esses controles em nenhuma unidade organizacional. Você pode optar por desativar esses controles antes da data de remoção.

- [SH.S3.4]: os buckets do S3 devem ter a criptografia no lado do servidor habilitada.
- [CT.S3.PR.7]: exija que um bucket do Amazon S3 tenha a criptografia do lado do servidor configurada.

Motivo da desativação

Desde 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 a criptografia SSE-S3 ou do lado do servidor com as chaves do AWS Key Management Service (AWS KMS) (SSE-KMS) configuradas.

Versão 3.2 da zona de pouso do AWS Control Tower

16 de junho de 2023

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 3.2. Consulte informações em Atualizar a zona de pouso).

A versão 3.2 da zona de pouso do AWS Control Tower traz os controles que fazem parte do padrão AWS Security Hub gerenciado por serviços: AWS Control Tower para disponibilidade geral. Ele introduz a capacidade de visualizar o status de desvio dos controles que fazem parte desse padrão no console do AWS Control Tower.

Essa atualização inclui uma nova função vinculada ao serviço (SLR), chamada de Torre. AWSService RoleFor AWSControl Essa função auxilia o AWS Control Tower criando uma regra EventBridge gerenciada, chamada de AWSControlTowerManagedRuleem cada conta membro. Essa regra gerenciada coleta eventos de AWS Security Hub busca, com o AWS Control Tower que pode determinar o desvio do controle.

Essa regra é a primeira regra gerenciada a ser criada pelo 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 campo `managed-by` for preenchido, ele mostrará a entidade principal do serviço AWS Control Tower.

Anteriormente, o 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 um ambiente com várias AWS contas. O novo perfil fornece permissões de escopo reduzido que permitem especificamente: criar a regra gerenciada nas contas-membros, manter a regra gerenciada, publicar notificações de segurança por meio do SNS e verificar o desvio. Para obter mais informações, consulte AWSServiceRoleForAWSControlTorre.

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 do controle do Security Hub (na zona de pouso 3.2 e posterior), o AWS Control Tower recebe uma atualização de status diária do Security Hub. Embora os controles estejam ativos

em todas as regiões governadas, o AWS Control Tower envia os eventos AWS Security Hub Finding somente para a região de origem da AWS Control Tower. Consulte mais informações em Security Hub control drift reporting.

Atualização do controle de negação de região

Essa versão da zona de pouso também inclui uma atualização para o controle de negação de região.

Serviços globais e APIs adicionados

- Gerenciamento de Faturamento e Custos da AWS (`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:*`)
- Pagamentos da Amazon (`payments:*`)
- AWS Configurações fiscais (`tax:*`)

Serviços globais e APIs removidos

- Remoção de `s3:GetAccountPublic` porque não é uma ação válida.
- Remoção de `s3:PutAccountPublic` porque não é uma ação válida.

AWS Control Tower gerencia contas com base em ID

14 de junho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora cria e gerencia contas que você cria no Account Factory rastreando o ID da AWS 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 `DescribeCreateAccountStatus`. Esse conjunto de permissões faz parte do perfil de Administrador e é concedido automaticamente quando um solicitante assume esse perfil. Se você delegar permissão para provisionar contas, talvez seja necessário adicionar essas permissões diretamente aos solicitantes da conta.

Controles de detecção adicionais do Security Hub disponíveis na biblioteca de controles do AWS Control Tower

12 de junho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower adicionou dez novos controles de AWS Security Hub detetive à 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 SageMaker AI e. AWS WAF Esses novos controles ajudam a aprimorar seu procedimento de governança atendendo aos objetivos de controle, como Estabelecer registro em log e monitoramento, Limitar o acesso à rede e Criptografar dados em repouso.

Esses controles agem como parte do Padrão gerenciado por serviços do Security Hub: AWS Control Tower, depois que você os habilita em qualquer UO específica.

- [sh.Account.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS
- [ELA. APIGateway.8] As rotas do API Gateway devem especificar um tipo de autorização
- [ELA. APIGateway.9] O registro de acesso deve ser configurado para os estágios V2 do API Gateway
- [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
- [SH.ELB.1]: o Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS.
- [SH.Redshift.10]: os clusters do Redshift devem ser criptografados em repouso.
- [ELA. SageMaker.2] As instâncias do notebook SageMaker AI devem ser iniciadas em uma VPC personalizada

- [ELA. SageMaker.3] Os usuários não devem ter acesso root às instâncias do notebook SageMaker AI
- [SH.WAF.10] Uma ACL WAFV2 da web deve ter pelo menos uma regra ou grupo de regras

Os novos controles de AWS Security Hub detetive estão disponíveis em todos os Regiões da AWS lugares onde o AWS Control Tower está disponível. Consulte mais detalhes sobre esses controles em Controls that apply to Service-Managed Standard: AWS Control Tower.

AWS Control Tower publica tabelas de metadados de controle

7 de junho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora fornece tabelas completas de metadados de controle como parte da documentação publicada. Ao trabalhar com o controle APIs, você pode consultar a API ControlIdentifier de cada controle, que é um ARN exclusivo associado a cada um. Região da AWS As tabelas incluem os frameworks 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 Padrão gerenciado por serviço do AWS Security Hub : AWS Control Tower. Consulte detalhes completos em Tables of control metadata.

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 o Account Factory Customization

6 de junho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower oferece suporte em uma única região para o Terraform por meio do Account Factory Customization (AFC). A partir desse lançamento, é possível usar o AWS Control Tower e o Service Catalog juntos para definir esquemas de contas do AFC no Terraform Open Source. Você pode personalizar seus recursos novos e existentes antes Contas da AWS de provisionar recursos no AWS Control Tower. Por padrão, esse recurso permite implantar e atualizar contas, com o Terraform, na sua região de origem do AWS Control Tower.

Um esquema de conta descreve os recursos e configurações específicos que são necessários quando uma Conta da AWS é provisionada. 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 do Terraform funcione com o Service Catalog. Esse processo de configuração único leva alguns minutos. Depois disso, é possível definir seus requisitos de conta personalizados no Terraform e, depois, implantar suas contas com o fluxo de trabalho bem definido do Account Factory do AWS Control Tower. Os clientes que preferem trabalhar com o Terraform podem utilizar a personalização de conta do AWS Control Tower em grande escala com o AFC e ter acesso imediato a cada conta após o provisionamento.

Para saber como criar essas personalizações, consulte Creating Products e Getting started with Terraform open source na documentação do Service Catalog. Esse recurso está disponível em todos os Regiões da AWS lugares onde o AWS Control Tower está disponível.

AWS Autogerenciamento do IAM Identity Center disponível para landing zone

6 de junho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece uma opção de provedor de identidades para uma zona de pouso do AWS Control Tower, que você pode definir durante a configuração ou atualização. Por padrão, a landing zone aceita usar o AWS IAM Identity Center, de acordo com as diretrizes de melhores práticas definidas em Organizando seu AWS ambiente usando várias contas. Agora você tem três alternativas:

- Você pode aceitar o padrão e permitir que o AWS Control Tower configure e gerencie o Centro de Identidade do AWS IAM para você.
- Você pode optar por autogerenciar o AWS IAM Identity Center para refletir seus requisitos comerciais específicos.
- Opcionalmente, você pode trazer e autogerenciar um provedor de identidades de terceiros, conectando-o por meio do Centro de Identidade do IAM, se necessário. Você deve usar a opção de provedor de identidade se seu ambiente regulatório exigir o uso de um provedor específico ou se você operar em um Regiões da AWS local onde o AWS IAM Identity Center não esteja disponível.

Para obter mais informações, consulte Orientações sobre o Centro de Identidade do IAM.

A seleção de provedores de identidade no nível da conta não é permitida. Esse recurso se aplica somente à zona de pouso como um todo. A opcionalidade do provedor de identidade do AWS Control Tower está disponível em todos os Regiões da AWS lugares onde o AWS Control Tower está disponível.

O AWS Control Tower aborda a governança mista para OUs

1.º de junho de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Com esse lançamento, o AWS Control Tower impede a implantação de controles em uma unidade organizacional (UO), se essa UO estiver em um estado de governança mista. A governança mista ocorre em uma OU se as contas não forem atualizadas depois que o AWS Control Tower estender a governança para uma nova Região da AWS ou remover a governança. Esse lançamento ajuda você a manter as contas-membros dessa UO em conformidade uniforme. Para obter mais informações, consulte Evitar governança mista ao configurar regiões.

Controles proativos adicionais disponíveis

19 de maio de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower está adicionando 28 novos controles proativos para ajudar a administrar o ambiente de várias contas e a cumprir 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 AI, SageMaker Amazon API Gateway e Amazon Relational Database Service (RDS).

Os controles proativos são suportados em todos os comerciais em Regiões da AWS que o AWS Control Tower está disponível.

OpenSearch Serviço Amazon

- [CT.OPENSEARCH.PR.1]: exija um domínio do Elasticsearch para criptografar dados em repouso.

- [CT.OPENSEARCH.PR.2]: exija que um domínio do Elasticsearch seja criado em uma Amazon VPC especificada pelo usuário.
- [CT.OPENSEARCH.PR.3]: exija 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] Exija que um domínio do Elasticsearch Service use .2 TLSv1
- [CT.OPENSEARCH.PR.9] Exigir um domínio do OpenSearch Amazon Service para criptografar dados em repouso
- [CT.OPENSEARCH.PR.10] Exija que um domínio do Amazon Service seja criado em uma OpenSearch Amazon VPC especificada pelo usuário
- [CT.OPENSEARCH.PR.11] Exigir um domínio do OpenSearch Amazon Service para criptografar dados enviados entre os nós
- [CT.OPENSEARCH.PR.12] Exigir um domínio do Amazon Service para enviar registros de erros para o OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.13] Exigir um domínio do Amazon Service para enviar registros de auditoria para o OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.14] Exija que um domínio do OpenSearch Amazon Service tenha reconhecimento de zona e pelo menos três nós de dados
- [CT.OPENSEARCH.PR.15] Exija um domínio do OpenSearch Amazon Service para usar um controle de acesso refinado
- [CT.OPENSEARCH.PR.16] Exigir um domínio do Amazon Service para usar .2 OpenSearch TLSv1

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Exija que um grupo do Amazon Auto EC2 Scaling tenha várias zonas de disponibilidade

- [CT.AUTOSCALING.PR.2] Exija uma configuração de lançamento de grupo do Amazon Auto EC2 Scaling para configurar instâncias da Amazon para EC2 IMDSv2
- [CT.AUTOSCALING.PR.3] Exija que uma configuração de lançamento do Amazon Auto EC2 Scaling tenha um limite de resposta de metadados de salto único
- [CT.AUTOSCALING.PR.4] Exija que um grupo do Amazon Auto EC2 Scaling associado a um Amazon Elastic Load Balancing (ELB) tenha as verificações de saúde do ELB ativadas
- [CT.AUTOSCALING.PR.5] Exija que uma configuração de lançamento de grupo do Amazon Auto EC2 Scaling não tenha instâncias da Amazon com endereços IP públicos EC2
- [CT.AUTOSCALING.PR.6] Exija que qualquer grupo do Amazon Auto EC2 Scaling use vários tipos de instância
- [CT.AUTOSCALING.PR.8] Exija que um grupo do Amazon Auto EC2 Scaling tenha modelos de lançamento configurados EC2

SageMaker Inteligência Artificial da Amazon

- [CT.SAGEMAKER.PR.1] Exija uma instância de notebook Amazon SageMaker AI para impedir o acesso direto à Internet
- [CT.SAGEMAKER.PR.2] Exija que as instâncias do notebook Amazon AI sejam implantadas em uma SageMaker Amazon VPC personalizada
- [CT.SAGEMAKER.PR.3] Exija que as instâncias do notebook Amazon AI tenham acesso root não permitido SageMaker

Amazon API Gateway

- [CT.APIGATEWAY.PR.5]: exija rotas de Websocket e HTTP do Amazon API Gateway V2 para especificar um tipo de autorização.

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25]: exija que um cluster de banco de dados do Amazon RDS tenha o registro em log configurado.

Consulte mais informações em Proactive controls.

Controles EC2 proativos atualizados da Amazon

2 de maio de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower atualizou dois controles proativos: CT.EC2.PR.3 and CT.EC2.PR.4.

Para o atualizado CT.EC2.PR.3 controle, qualquer AWS CloudFormation implantação que faça referência a uma lista de prefixos para um recurso do grupo de segurança é bloqueada de ser implantada, a menos que seja para a porta 80 ou 443.

Para o atualizado CT.EC2.PR.4 controle, qualquer AWS CloudFormation implantação que faça referência a uma lista de prefixos para um recurso de grupo de segurança será 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 disponíveis

19 de abril de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS 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 (N. da Califórnia), que está ativa por padrão.

Alguns controles no AWS Control Tower não operam em algumas dessas Regiões da AWS adicionais onde o AWS Control Tower está disponível, porque essas regiões não são compatíveis com a funcionalidade subjacente necessária. Para obter detalhes, consulte Limitações de controle.

Dentre essas novas regiões, o CfCT não está disponível na região Ásia-Pacífico (Jacarta e Osaka). A disponibilidade em outros Regiões da AWS permanece inalterada.

Consulte mais informações sobre como o AWS Control Tower gerencia as limitações de regiões e controles em Considerações sobre como ativar as regiões opcionais da AWS.

Os VPCe endpoints exigidos pela AFT não estão disponíveis na região do Oriente Médio (Bahrein). Os clientes que implantam o AFT nesta região devem implantar com o parâmetro `aft_vpc_endpoints=false`. Consulte mais informações no parâmetro do arquivo README.

O AWS Control Tower VPCs tem duas zonas de disponibilidade na região Oeste dos EUA (Norte da Califórnia)`us-west-1`, devido a uma limitação na Amazon EC2. Na região Oeste dos EUA (N. da Califórnia), seis sub-redes são divididas em duas zonas de disponibilidade. Para obter mais informações, consulte Visão geral do AWS Control Tower e VPCs.

A AWS Control Tower adicionou novas permissões para permitir `AWSControlTowerServiceRolePolicy` que a AWS Control Tower faça chamadas para`EnableRegion`,`ListRegions`, e `GetRegionOptStatus` APIs implementadas pelo serviço de gerenciamento de AWS contas, para Regiões da AWS disponibilizar essas permissões adicionais 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.

Rastreamento de solicitações de personalização de conta do Account Factory for Terraform (AFT)

16 de fevereiro de 2023

O AFT permite o rastreamento de solicitações de personalização de conta. Toda vez que você envia uma solicitação de personalização de conta, o AFT gera um token de rastreamento exclusivo que passa por uma máquina de AWS Step Functions estado de personalização do AFT, 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, é possível ver as cargas úteis que acompanham o token, para que você possa rastrear sua solicitação de personalização de conta em todo o fluxo de trabalho do AFT. Consulte mais informações sobre o AFT em Overview of 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 AWS Step Functionsé no Guia do AWS Step Functions desenvolvedor

Versão 3.1 da zona de pouso do AWS Control Tower

9 de fevereiro de 2023

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 3.1. Consulte informações em Atualizar a zona de pouso)

A versão 3.1 da zona de pouso do AWS Control Tower inclui as seguintes atualizações:

- Com esse lançamento, o AWS Control Tower desativa o registro em log de acesso desnecessário para o bucket de registro em log de acesso, que é o bucket do Amazon S3 em que os logs de acesso são armazenados na conta de arquivamento de logs, enquanto continua habilitando o registro em log 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 Suporte Planos AWS Artifact e.
- A desativação do registro em log de acesso ao servidor para o bucket de registro em log de acesso do AWS Control Tower faz com que o Security Hub crie uma descoberta para o bucket de registro em log de acesso da conta de arquivamento de logs, devido a uma regra do AWS Security Hub : [S3.9] O registro em log de acesso ao servidor do bucket do S3 deve ser habilitado. Em alinhamento com o Security Hub, recomendamos que você suprima essa descoberta específica, conforme declarado na descrição dessa regra no Security Hub. Consulte informações adicionais sobre descobertas suprimidas.
- O registro em log de acesso para o bucket de registro em log (regular) na conta de arquivamento de logs permanece inalterado na versão 3.1. De acordo com as práticas recomendadas, os eventos de acesso desse bucket são registrados como entradas de log no bucket de registro em log de acesso. Consulte mais informações sobre o registro em log de acesso em Registrar em log as solicitações com registro em log de acesso ao servidor na documentação do Amazon S3.
- Fizemos uma atualização no controle de negação de região. Essa atualização permite ações de mais serviços globais. Para obter detalhes sobre esse SCP, consulte Negar acesso AWS com base na solicitação Região da AWS e Controles que aprimoram a proteção da residência de dados.

  Serviços globais adicionados:

  - AWS Gerenciamento de contas (`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:*`)
- Centro de Identidade do IAM (`sso:*`)
- AWS Support App (`supportapp:*`)
- Suporte Planos (`supportplans:*`)
- AWS Sustentabilidade (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Informações do fornecedor () `vendor-insights:ListEntitledSecurityProfiles`

Controles proativos disponíveis ao público

24 de janeiro de 2023

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

Os controles proativos opcionais, anunciados anteriormente no status de prévia, já estão disponíveis ao público. 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 no ambiente. Para obter mais informações, consulte Controles abrangentes auxiliam no provisionamento e gerenciamento de recursos da AWS.

De janeiro a dezembro de 2022

Em 2022, o AWS Control Tower lançou as seguintes atualizações:

- Operações de conta simultâneas
- Account Factory Customization (AFC)
- Controles abrangentes auxiliam no provisionamento e gerenciamento de recursos da AWS
- Status de conformidade visível para todas as regras do AWS Config

- API para controles e um novo recurso da AWS CloudFormation
- O CfCT permite a exclusão do conjunto de pilhas
- Retenção de logs personalizada
- Reparo de desvio de perfil disponível
- Versão 3.0 da zona de pouso do AWS Control Tower
- A página Organização combina visualizações OUs e contas
- Inscrição e atualização mais fáceis para contas-membros individuais
- AFT permite a personalização automatizada para contas compartilhadas do AWS Control Tower
- Operações simultâneas para todos os controles opcionais
- Contas de segurança e de registro em log existentes
- Versão 2.9 da zona de pouso do AWS Control Tower
- Versão 2.8 da zona de pouso do AWS Control Tower

Operações de conta simultâneas

16 de dezembro de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora permite ações simultâneas no Account Factory. É possível 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 as 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 (UO) inteira.

Account Factory Customization (AFC)

28 de novembro de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O Account Factory Customization permite que você personalize contas novas e existentes no console do AWS Control Tower. Esses novos recursos de personalização oferecem a flexibilidade de definir esquemas de conta, que são AWS CloudFormation modelos contidos em um produto especializado do Service Catalog. Os esquemas fornecem recursos e configurações totalmente

personalizados. Você também pode optar por usar esquemas predefinidos, criados e gerenciados por parceiros da AWS , que ajudam a personalizar contas para casos de uso específicos.

Anteriormente, o Account Factory do AWS Control Tower não permitia a personalização de contas no console. Com essa atualização do Account Factory, é possível 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, inscrever outras AWS contas na AWS Control Tower e atualizar as contas existentes da AWS Control Tower.

Ao provisionar, inscrever ou atualizar uma conta no Account Factory, você seleciona o esquema a ser implantado. Esses recursos especificados no esquemas são provisionados na conta. Quando a conta termina de ser criada, todas as configurações personalizadas ficam disponíveis para uso imediato.

Para começar a personalizar contas, é possível definir os recursos para o caso de uso pretendido em um produto do Service Catalog. Você também pode selecionar soluções gerenciadas por parceiros na AWS Getting Started Library. Para obter mais informações, consulte Personalizar contas com Account Factory Customization (AFC).

Controles abrangentes auxiliam no provisionamento e gerenciamento de recursos da AWS

28 de novembro de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora oferece suporte ao gerenciamento abrangente de controles, incluindo controles proativos novos e 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 estão em conformidade com os controles ativados no ambiente.

Mais de 130 novos controles proativos ajudam você a cumprir objetivos políticos específicos para seu ambiente da AWS Control Tower; a atender aos requisitos das estruturas de conformidade padrão do setor; e a governar as interações da AWS Control Tower em mais de vinte outros serviços. AWS

A biblioteca de controles do AWS Control Tower classifica esses controles de acordo com os AWS serviços e recursos associados. Consulte mais detalhes em Proactive controls.

Com essa versão, o AWS Control Tower também é integrado AWS Security Hub, por meio do novo padrão gerenciado por serviços do Security Hub: o AWS Control Tower, que suporta o padrão AWS Foundational Security Best Practices (FSBP). Você pode ver mais de 160 controles do Security Hub junto com os controles do AWS Control Tower no console e obter uma pontuação de segurança do Security Hub para o ambiente do AWS Control Tower. Consulte mais informações em Security Hub controls.

Status de conformidade visível para todas as regras do AWS Config

18 de novembro de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora exibe o status de conformidade de todas as AWS Config regras implantadas em unidades organizacionais registradas na AWS Control Tower. Você pode ver o status de conformidade de todas AWS Config as regras que afetam suas contas na AWS Control Tower, inscritas ou não inscritas, sem sair do console do AWS Control Tower. Os clientes podem optar por configurar regras do Config, chamadas de controles de detetive, no AWS Control Tower ou configurá-las diretamente por meio do serviço. AWS Config As regras implantadas por AWS Config são mostradas, junto com as regras implantadas pelo AWS Control Tower.

Anteriormente, AWS Config as regras implantadas por meio do AWS Config serviço não eram visíveis no console do AWS Control Tower. Os clientes precisavam acessar o AWS Config serviço para identificar regras não compatíveis. AWS Config Agora você pode identificar qualquer AWS Config regra não compatível no console do AWS Control Tower. Para ver o status de conformidade de todas as regras do Config, acesse a página Detalhes da conta no console do AWS Control Tower. Você verá uma lista mostrando o status de conformidade dos controles gerenciados pelas regras do Config e do AWS Control Tower implantadas fora do AWS Control Tower.

API para controles e um novo recurso da AWS CloudFormation

1º de setembro de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora permite o gerenciamento programático de controles, também conhecido como barreiras de proteção, por meio de um conjunto de chamadas de API. Um novo recurso da AWS CloudFormation é compatível com a funcionalidade da API para controles. Para obter mais detalhes, consulte Automatizar 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 dos controles do aplicativo na biblioteca do AWS Control Tower. Eles APIs incluem suporte para AWS CloudFormation, para que você possa gerenciar AWS recursos como infrastructure-as-code (IaC). O AWS 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 contas ou faz alterações nas contas existentes.

APIs incluído nesta versão

- EnableControl— Essa chamada de API ativa um controle. Ele inicia uma operação assíncrona que cria recursos da AWS na unidade organizacional especificada e nas contas que ela contém.
- DisableControl— Essa chamada de API desativa um controle. Ele inicia uma operação assíncrona que exclui recursos da AWS na unidade organizacional especificada e nas contas que ela contém.
- GetControlOperation— Retorna o status de uma determinada DisableControloperação EnableControlou operação.
- ListEnabledControls— Lista os controles habilitados 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 Guia do usuário do AWS Control Tower.

O CfCT permite a exclusão do conjunto de pilhas

26 de agosto de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O Customizations for AWS Control Tower (CfCT) agora permite a 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, TODOS os recursos que começam com o prefixo `CustomControlTower-`, que têm a tag de chave `Key:AWS_Solutions, Value: CustomControlTowerStackSet` associada e que não são declarados no arquivo de manifesto, são preparados para exclusão.

Retenção de logs personalizada

15 de agosto de 2022

(Atualização necessária para a zona de pouso do AWS Control Tower. Consulte informações em Atualizar a zona de pouso)

O AWS 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 É possível personalizar a 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 a retenção de logs, as configurações padrão são de um ano para registro em log de conta padrão e 10 anos para registro em log de acesso.

Esse recurso está disponível para clientes existentes por meio do AWS Control Tower quando você atualiza ou repara a zona de pouso, e para novos clientes por meio do processo de configuração do AWS Control Tower.

Reparo de desvio de perfil disponível

11 de agosto de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora permite o reparo em caso de desvio de perfil. É possível restaurar um perfil necessário sem um reparo completo da zona de pouso. Se esse tipo de reparo de desvio for necessário, a página de erro do console fornece etapas para restaurar o perfil, para que a zona de pouso esteja novamente disponível.

Versão 3.0 da zona de pouso do AWS Control Tower

29 de julho de 2022

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 3.0. Consulte informações em Atualizar a zona de pouso)

A versão 3.0 da zona de pouso do AWS Control Tower inclui as seguintes atualizações:

- A opção de escolher trilhas em nível organizacional ou optar por não participar das AWS CloudTrail CloudTrail trilhas gerenciadas pelo 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 na sua região de origem.
- Uma atualização do controle de negação de região.
- Uma atualização da política gerenciada, AWSControlTowerServiceRolePolicy.
- Não criamos mais a função do IAM `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 da organização, criamos apenas um na conta de gerenciamento.

As seções a seguir fornecem mais detalhes sobre cada recurso novo.

CloudTrail Trilhas em nível organizacional no AWS Control Tower

Com a versão 3.0 da zona de pouso, o AWS Control Tower agora permite trilhas do AWS CloudTrail no nível da organização.

Ao atualizar sua zona de pouso da AWS Control Tower para a versão 3.0, você tem a opção de selecionar AWS CloudTrail trilhas no nível da organização como sua preferência de registro ou optar por não receber CloudTrail trilhas gerenciadas pela AWS Control Tower. Quando você atualiza para a versão 3.0, o AWS Control Tower exclui as trilhas existentes no nível da conta para contas inscritas após um período de espera de 24 horas. O AWS Control Tower não exclui trilhas no nível da conta para contas não inscritas. No caso improvável de a atualização da zona de pouso não ser bem-sucedida, mas a falha ocorrer depois que o AWS Control Tower já tiver criado a trilha no nível da organização, você poderá incorrer em cobranças duplicadas pelas trilhas no nível da organização e da conta, até que a operação de atualização seja concluída com sucesso.

A partir da landing zone 3.0, o AWS Control Tower não oferece mais suporte a trilhas gerenciadas em nível de conta. AWS 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 CloudTrail trilhas em nível de conta gerenciadas pelo AWS Control Tower.

Nenhum dado de registro em log é perdido dos logs de conta agregados, porque os logs permanecem no bucket existente do Amazon S3, onde estão armazenados. Somente as trilhas são excluídas, não os logs existentes. Se você selecionar a opção de adicionar trilhas no nível da organização, o AWS Control Tower abrirá um novo caminho para uma nova pasta dentro do bucket do Amazon S3 e continuará enviando informações de registro em log para esse local. Se você optar por não participar das trilhas gerenciadas pelo AWS Control Tower, os logs existentes permanecerão no bucket, inalterados.

Convenções de nomenclatura de caminhos para armazenamento de logs

- Os logs de trilha da conta são armazenados com um caminho deste formato: `/org id/AWSLogs/…`
- Os logs de trilha 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 em nível organizacional é diferente do caminho padrão para uma trilha em nível organizacional 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 no nível de conta, recomendamos que você crie as trilhas antes de concluir a atualização para a versão 3.0 da zona de pouso do AWS Control Tower, para começar o registro em log 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 optar por aceitar ou cancelar trilhas no nível da organização, sempre que atualizar a zona de pouso.

Se os logs forem gerenciados por um serviço de terceiros, forneça o nome do novo caminho para o serviço.

> **Note**
>
> Para zonas de pouso na versão 3.0 ou posterior, AWS CloudTrail trilhas em nível de conta não são suportadas pelo AWS Control Tower. É possível criar e manter suas próprias trilhas no nível da conta a qualquer momento, ou pode optar por trilhas no nível da organização gerenciadas pelo AWS Control Tower.

AWS Config Registre recursos somente na região de origem

Na versão 3.0 da zona de pouso, o AWS Control Tower atualizou a configuração da linha de base para o AWS Config a fim de registrar recursos globais somente na região de origem. Depois de atualizar para a versão 3.0, a gravação de recursos globais é ativada somente na região de origem.

Essa configuração é considerada uma prática recomendada. É recomendado por AWS Security Hub e e AWS Config 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 serviço da AWS , um item de configuração era criado para cada item em cada região administrada.

Dois novos controles de detecção para registro em log do AWS CloudTrail

Como parte da mudança nas AWS CloudTrail trilhas em nível organizacional, o AWS Control Tower está introduzindo dois novos controles de detetive que verificam se está habilitado. CloudTrail O primeiro controle tem orientação Obrigatória e é habilitado na UO de segurança durante as atualizações de configuração ou da zona de pouso da versão 3.0 e posterior. 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 o CloudTrail Lake ativado

Controle altamente recomendado: detecte se uma conta tem AWS CloudTrail ou o CloudTrail Lake ativado

Consulte mais informações sobre os novos controles em The AWS Control Tower controls library.

Uma atualização do controle de negação de região

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",
```

Vídeo de demonstração

Este vídeo (3:07) descreve como atualizar a zona de pouso atual do 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.

Video Walkthrough of Update an Existing AWS Control Tower Landing Zone to Landing Zone 3.

A página Organização combina visualizações OUs e contas

18 de julho de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

A nova página da 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 aninhadas OUs. Você pode agir em agrupamentos de recursos. É possível 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 registradas OUs, 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-membros individuais

31 de maio de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora oferece um recurso aprimorado de atualizar e inscrever contas-membros individualmente. Cada conta mostra quando está disponível para uma atualização, para que você possa garantir mais facilmente que suas contas-membros incluam a configuração mais recente. É possível atualizar a zona de pouso, corrigir o desvio da conta ou inscrever uma conta em uma UO registrada, em algumas etapas simplificadas.

Quando você atualiza uma conta, não é necessário incluir toda a unidade organizacional (UO) da conta em cada ação de atualização. Como resultado, o tempo necessário para atualizar uma conta individual é bastante reduzido.

Você pode inscrever contas no AWS Control Tower OUs com mais ajuda do console do 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 o perfil `AWSControlTowerExecution`. Depois, você pode escolher qualquer UO registrada e inscrever a conta nela selecionando o botão Inscrever.

Separamos a funcionalidade Inscrever conta do fluxo de trabalho Criar conta no Account Factory para distinguir melhor esses processos semelhantes e ajudar a evitar erros de configuração ao inserir as informações da conta.

AFT permite a personalização automatizada para contas compartilhadas do AWS Control Tower

27 de maio de 2022

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O Account Factory for Terraform (AFT) agora pode personalizar e atualizar programaticamente qualquer uma das suas contas gerenciadas pelo AWS Control Tower, incluindo a conta de gerenciamento, a conta de auditoria e a conta de arquivamento de logs, junto com suas contas

inscritas. É possível centralizar a personalização da conta e o gerenciamento de atualizações e, ao mesmo tempo, proteger a segurança das configurações da conta, porque você define o escopo do perfil que executa o trabalho.

A AWSAFTExecutionfunção existente agora implanta personalizações em todas as contas. Você pode configurar permissões do IAM 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 nesse perfil para usuários confiáveis. Como prática recomendada, é aconselhável restringir as permissões às necessárias para implantar as personalizações necessárias.

A AFT agora cria a nova AWSAFTServicefunção para implantar recursos da AFT 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 gerenciadas do AWS Control Tower não são provisionadas pela fábrica de contas, portanto, elas não têm produtos provisionados correspondentes. 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

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora permite operações simultâneas para controles preventivos, bem como para controles de detecção.

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. É possível habilitar vários controles opcionais sem esperar que as operações de controle individuais sejam concluídas. Os únicos horários restritos são quando o AWS Control Tower está no processo de configuração da zona de pouso ou ao estender a governança a uma nova organização.

Funcionalidade compatível apenas com controles preventivos:

- Aplique e remova diferentes controles preventivos na mesma UO.
- Aplique e remova diferentes controles preventivos em diferentes OUs, simultaneamente.
- Aplique e remova o mesmo controle preventivo em vários OUs, simultaneamente.
- É possível aplicar e remover controles preventivos e de detecção simultaneamente.

Você pode experimentar essas melhorias de controle simultâneo em todas as versões lançadas do AWS Control Tower.

Quando você aplica controles preventivos ao aninhado OUs, os controles preventivos afetam todas as contas e estão OUs aninhadas na OU de destino, mesmo que essas contas não OUs estejam registradas no AWS Control Tower. Os controles preventivos são implementados usando as Políticas de Controle de Serviços (SCPs), que fazem parte de AWS Organizations. Os controles de detetive são implementados usando AWS Config regras. As barreiras de proteção permanecem em vigor à medida que você cria contas ou faz alterações em contas existentes, e o AWS Control Tower fornece um relatório resumido de como cada conta está em conformidade com as políticas habilitadas. Consulte uma lista completa dos controles disponíveis em The AWS Control Tower controls library.

Contas de segurança e de registro em log existentes

16 de maio de 2022

(Disponível durante a configuração inicial.)

O AWS Control Tower agora oferece a opção de você especificar uma AWS conta existente 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 o 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 na zona de pouso. A conta de registro em log, chamada de conta de arquivamento de logs por padrão, funciona como um repositório. Ela armazena logs de atividades de API e configurações de recursos de todas as contas na zona de pouso.

Ao trazer suas contas existentes de segurança e de registro em log, é mais fácil estender a governança do AWS Control Tower para suas organizações existentes ou migrar de uma zona de pouso alternativa para o AWS Control Tower. A opção de usar contas existentes é exibida durante a configuração inicial da zona de pouso. Ela inclui verificações durante o processo de configuração, que garantem a implantação bem-sucedida. O AWS Control Tower implementa os perfil e os controles necessários nas contas existentes. Ele não remove nem mescla nenhum recurso ou dado existente nessas contas.

Limitação: Se você planeja trazer AWS contas existentes para a AWS Control Tower como contas de auditoria e arquivamento de registros, e se essas contas tiverem AWS Config recursos existentes, você deverá excluir os AWS Config recursos existentes antes de poder cadastrá-las na AWS Control Tower.

Versão 2.9 da zona de pouso do AWS Control Tower

22 de abril de 2022

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 2.9. Consulte informações em Atualizar a zona de pouso)

A versão 2.9 da zona de pouso do AWS Control Tower atualiza o encaminhador de notificações do Lambda para usar o runtime do Python versão 3.9. Essa atualização aborda a desativação da versão 3.6 do Python, planejada para julho de 2022. Consulte as informações mais recentes na página de desativação do Python.

Versão 2.8 da zona de pouso do AWS Control Tower

10 de fevereiro de 2022

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 2.8. Consulte informações em Atualizar a zona de pouso)

A versão 2.8 da zona de pouso do AWS Control Tower adiciona uma funcionalidade que se alinha às atualizações recentes de AWS Foundational Security Best Practices.

Nesse lançamento:

- O registro em log de acesso é configurado para o bucket de log de acesso na conta de arquivamento de logs, para acompanhar o acesso ao bucket de log de acesso existente do S3.
- Suporte adicionado para políticas de ciclo de vida. 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 o AWS Control Tower para usar o AWS Service Linked Role (SLR) fornecido por AWS Config, em todas as contas gerenciadas (sem incluir a conta de gerenciamento), para que você possa configurar e gerenciar as regras do Config de acordo AWS Config com as melhores práticas. Os clientes que não fizerem upgrade continuarão usando o perfil atual.
- Essa versão simplifica o processo de configuração do AWS Control Tower KMS para criptografar AWS Config dados e melhora as mensagens de status relacionadas. CloudTrail
- O lançamento inclui uma atualização do controle de negação de região, para permitir o recurso `route53-application-recovery` na região `us-west-2`.
- Atualização: em 15 de fevereiro de 2022, removemos a fila de mensagens não entregues das funções do AWS Lambda.

Outros detalhes:

- Se você desativar a zona de pouso, o AWS Control Tower não removerá o perfil vinculado ao serviço do AWS Config .
- Se você desprovisionar uma conta do Account Factory, o AWS Control Tower não removerá o perfil vinculado ao serviço do AWS Config .

Para atualizar a zona de pouso para 2.8, acesse a página Configurações de zona inicial, selecione a versão 2.8 e escolha Atualizar. Depois de atualizar a zona de pouso, você deve atualizar todas as contas que são administradas pelo AWS Control Tower, conforme indicado em Gerenciamento de atualizações de configuração no AWS Control Tower.

De janeiro a dezembro de 2021

Em 2021, o AWS Control Tower lançou as seguintes atualizações:

- Recursos de negação de região
- Atributos de residência de dados
- AWS Control Tower apresenta o provisionamento e a personalização de contas do Terraform
- Novo evento do ciclo de vida disponível
- O AWS Control Tower permite o aninhamento OUs
- Simultaneidade do controle de detecção
- Duas novas regiões disponíveis
- Desmarcação de região
- O AWS Control Tower funciona com sistemas de gerenciamento de AWS chaves
- Controles renomeados, funcionalidade inalterada
- O AWS Control Tower escaneia SCPs diariamente para verificar se há desvio
- Nomes OUs e contas personalizados
- Versão 2.7 da zona de pouso do AWS Control Tower
- Três novas AWS regiões disponíveis
- Administrar somente regiões selecionadas
- O AWS Control Tower agora estende a governança às existentes OUs em suas AWS organizações

- AWS Control Tower disponibiliza atualizações de contas em massa

Recursos de negação de região

30 de novembro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower.)

O AWS Control Tower agora fornece recursos de negação de regiões, que ajudam você a limitar o acesso a AWS serviços e operações para contas inscritas em seu ambiente do AWS Control Tower. O recurso de negação de região complementa os recursos existentes de seleção e desmarcação de regiões no AWS Control Tower. Em conjunto, esses recursos ajudam a lidar com questões regulatórias e de conformidade, ao mesmo tempo que equilibram os custos associados à expansão para outras regiões.

Por exemplo, AWS clientes na Alemanha podem negar acesso AWS a serviços em regiões fora da região de Frankfurt. Você pode selecionar regiões restritas durante o processo de configuração do AWS Control Tower ou na página Configurações de zona inicial. O recurso de negação de região é disponibilizado quando você atualiza a versão da zona de pouso do AWS Control Tower. Alguns AWS serviços estão isentos dos recursos de negação por região. Para saber mais, consulte Configure the Region deny control.

Atributos de residência de dados

30 de novembro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora oferece controles específicos para ajudar a garantir que todos os dados de clientes que você envie para AWS os serviços estejam localizados somente nas AWS regiões que você especificar. Você pode selecionar a AWS região ou regiões nas quais os dados do seu cliente são armazenados e processados. Para obter uma lista completa das AWS regiões em que o AWS Control Tower está disponível, consulte a tabela de AWS regiões.

Para controle granular, é possível aplicar controles adicionais, como Proibir conexões da Amazon Virtual Private Network (VPN) ou Proibir o acesso à internet para uma instância da Amazon VPC. É possível visualizar o status de conformidade dos controles no console do AWS Control Tower. Consulte uma lista completa dos controles disponíveis em The AWS Control Tower controls library.

AWS Control Tower apresenta o provisionamento e a personalização de contas do Terraform

29 de novembro de 2021

(Atualização opcional para a zona de pouso do AWS Control Tower)

Agora é possível usar o Terraform para provisionar e atualizar contas personalizadas por meio do AWS Control Tower, com o Account Factory for Terraform (AFT) do AWS Control Tower.

O AFT fornece um único pipeline de infraestrutura como código (IaC) do Terraform, que provisiona contas gerenciadas pelo 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 automatizado de criação de contas do AFT monitora até que o provisionamento da conta seja concluído e, depois, continua, acionando módulos 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 recursos do AFT, fornecidas AWS pelas personalizações comuns.

Comece a usar o Account Factory for Terraform do AWS Control Tower seguindo as etapas fornecidas no Guia do usuário do AWS Control Tower, Account Factory for Terraform (AFT) do AWS Control Tower, e baixando o AFT para sua instância do Terraform. O AFT é compatível com as distribuições Terraform Cloud, Terraform Enterprise e Terraform Open Source.

Novo evento do ciclo de vida disponível

18 de novembro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O `PrecheckOrganizationalUnit` evento registra se algum recurso impede o sucesso da tarefa de governança Extend, incluindo recursos aninhados OUs. Para obter mais informações, consulte `PrecheckOrganizationalUnit`.

O AWS Control Tower permite o aninhamento OUs

16 de novembro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora permite que você inclua o aninhado OUs como parte da sua landing zone.

O AWS 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 aninhado OUs, criar e registrar OUs como pai OUs e habilitar 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 nested OUs, você pode alinhar sua AWS Control Tower OUs à estratégia de AWS várias contas e reduzir o tempo necessário para habilitar controles em várias OUs, 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 pela OU de nível superior e depois descendo pela árvore. Para obter mais informações, consulte Expandir de uma estrutura de UO plana para uma estrutura de UO aninhada.
2. As contas diretamente em uma UO registrada são registradas automaticamente. As contas mais abaixo na árvore podem ser registradas registrando a UO principal imediata.
3. Os controles preventivos (SCPs) são herdados automaticamente na hierarquia; SCPs aplicados ao pai são herdados por todos os aninhados. OUs
4. Os controles Detective (regras de AWS configuração) NÃO são herdados automaticamente.
5. A conformidade com os controles de detecção é relatada por cada UO.
6. A variação do SCP 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).

Simultaneidade do controle de detecção

5 de novembro de 2021

(Atualização opcional para a zona de pouso do AWS Control Tower)

Os controles de detecção do AWS Control Tower agora são compatíveis com operações simultâneas para controles de detecção, melhorando a facilidade de uso e o desempenho. É possível habilitar

vários controles de detecção sem esperar que as operações de controle individuais sejam concluídas.

Funcionalidades compatíveis:

- Habilite diferentes controles de detecção na mesma UO (por exemplo, Detectar se a MFA para o usuário-raiz está habilitada e Detectar se o acesso público de gravação nos buckets do Amazon S3 é permitido).
- Ative diferentes controles de detetive em diferentes OUs, simultaneamente.
- As mensagens de erro da barreira de proteção foram aprimoradas para fornecer mais orientações para operações de simultaneidade de controle compatíveis.

Não compatível com esta versão:

- Não OUs há suporte para ativar o mesmo controle de detetive em vários ao mesmo tempo.
- A simultaneidade de controle preventivo não é permitida.

Você pode experimentar as melhorias de simultaneidade do controle de detecção 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 zona de pouso para aproveitar outros recursos, como seleção e desmarcação 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 do AWS Control Tower)

O AWS Control Tower agora está disponível em duas AWS regiões adicionais: América do Sul (São Paulo) e Europa (Paris). Essa atualização expande a disponibilidade do AWS Control Tower para 15 regiões da AWS .

Se você é iniciante no AWS Control Tower, pode iniciá-lo imediatamente em qualquer uma das regiões compatíveis. Durante a inicialização, é possível selecionar as regiões nas você quais deseja que o AWS Control Tower crie e controle seu ambiente de várias contas.

Se você já tem um ambiente do AWS Control Tower e deseja estender ou remover os recursos de governança do AWS Control Tower em uma ou mais regiões compatíveis, acesse a página

Configurações de zona inicial no painel do AWS Control Tower e selecione as regiões. Depois de atualizar a zona de pouso, você deve atualizar todas as contas que são administradas pelo AWS Control Tower.

Desmarcação de região

29 de julho de 2021

(Atualização opcional para a zona de pouso do AWS Control Tower)

A desmarcação de região do AWS Control Tower aprimora sua capacidade de gerenciar a área geográfica dos recursos do AWS Control Tower. É possível desmarcar regiões que você não gostaria mais que o AWS Control Tower administrasse. Esse recurso permite abordar questões regulatórias e de conformidade e, ao mesmo tempo, equilibrar os custos associados à expansão para outras regiões.

A desmarcação de região fica disponível quando você atualiza sua versão da zona de pouso do AWS Control Tower.

Quando você usa o Account Factory para criar uma conta ou inscrever uma conta-membro preexistente, ou quando seleciona Estender governança para inscrever contas em uma unidade organizacional preexistente, o AWS Control Tower implanta seus recursos de governança, que incluem registro em log, monitoramento e controles centralizados, nas regiões escolhidas nas contas. A opção de desmarcar uma região e remover a governança do AWS Control Tower dessa região remove essa funcionalidade de governança, mas não inibe a capacidade dos usuários de implantar AWS recursos ou cargas de trabalho nessas regiões.

O AWS Control Tower funciona com sistemas de gerenciamento de AWS chaves

28 de julho de 2021

(Atualização opcional para a zona de pouso do AWS Control Tower)

O AWS Control Tower oferece a opção de usar uma AWS chave do Key Management Service (AWS KMS). Uma chave é fornecida e gerenciada por você para proteger os serviços que o AWS Control Tower implanta, incluindo AWS CloudTrail AWS Config, e os dados associados do Amazon S3. AWS A criptografia KMS é um nível aprimorado de criptografia em relação à criptografia SSE-S3 que o AWS Control Tower usa por padrão.

A integração do suporte do AWS KMS ao AWS Control Tower está alinhada às melhores práticas de segurança AWS básicas, que recomendam uma camada adicional de segurança para seus arquivos de log confidenciais. Você deve usar chaves AWS gerenciadas pelo KMS (SSE-KMS) para criptografia em repouso. AWS O suporte à criptografia do KMS está disponível quando você configura uma nova zona de pouso ou quando atualiza sua zona de pouso existente do AWS Control Tower.

Para configurar essa funcionalidade, você pode selecionar Configuração da chave do KMS durante a configuração inicial da zona de pouso. Você pode escolher uma chave KMS existente ou selecionar um botão que o direciona para o console AWS KMS para criar uma nova. Você também tem a flexibilidade de mudar da criptografia padrão para SSE-KMS ou para uma chave de SSE-KMS diferente.

Para uma zona de pouso existente do AWS Control Tower, você pode realizar uma atualização para começar a usar as chaves do AWS KMS.

Controles renomeados, funcionalidade inalterada

26 de julho de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower está revisando determinados nomes e descrições de controles para melhor refletir as intenções de políticas do controle. Os nomes e as 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 detecção de “Não permitir” para “Detectar” porque o controle de detecção 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 as descrições dos controles foram revisados.

O AWS Control Tower escaneia SCPs diariamente para verificar se há desvio

11 de maio de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora executa escaneamentos automatizados diários de seu gerente SCPs para verificar se os controles correspondentes foram aplicados corretamente e se não foram

desviados. Se uma verificação descobrir um desvio, você receberá uma notificação. O AWS Control Tower envia apenas uma notificação por problema de desvio, portanto, se a sua zona de pouso já estiver em um estado de desvio, você não receberá notificações adicionais a menos que um novo item de desvio seja encontrado.

Nomes OUs e contas personalizados

16 de abril de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora permite que você personalize a nomenclatura da zona de pouso. Você pode manter os nomes que o AWS Control Tower recomenda para as unidades organizacionais (OUs) e contas principais, ou você pode modificar esses nomes 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 à orientação de melhores práticas de AWS 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 UO anteriormente conhecida como UO principal agora é chamada de UO de segurança, e a UO anteriormente conhecida como UO personalizada agora é chamada de UO de sandbox. Fizemos essa alteração para melhorar nosso alinhamento com as diretrizes gerais de práticas recomendadas da AWS para nomenclatura.

Os novos clientes verão esses novos nomes de UO. Os clientes existentes continuarão vendo os nomes originais deles OUs. 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 do AWS Control Tower e selecione Set up landing zone no canto superior direito. Consulte mais informações lendo sobre como planejar sua zona de pouso do AWS Control Tower.

Versão 2.7 da zona de pouso do AWS Control Tower

8 de abril de 2021

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 2.7. Consulte informações em Atualizar a zona de pouso)

Com a versão 2.7 do AWS Control Tower, o AWS Control Tower introduz quatro novos controles preventivos obrigatórios de arquivamento de logs que implementam políticas somente nos recursos do AWS Control Tower. Ajustamos a orientação sobre os quatro controles existentes de arquivamento de logs de obrigatórios para eletivos, porque eles definem políticas para recursos fora do AWS Control Tower. Essa mudança e expansão de controle permitem separar a governança do arquivamento de logs para recursos dentro do AWS Control Tower da governança de recursos fora do 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 arquivos de AWS registros. Os ambientes existentes do AWS Control Tower manterão esses quatro controles alterados habilitados automaticamente, para garantir a consistência do ambiente. No entanto, esses controles eletivos agora podem ser desabilitados. Os novos ambientes do AWS Control Tower devem habilitar todos os controles eletivos. Os ambientes existentes devem desabilitar os controles anteriormente obrigatórios antes de adicionar criptografia aos buckets do Amazon S3 que não são implantados pelo AWS Control Tower.

Novos controles obrigatórios:

- Proibir alterações na configuração de criptografia dos buckets do S3 criados pelo AWS Control Tower no arquivamento de logs
- Proibir alterações na configuração de registro em log dos buckets do S3 criados pelo AWS Control Tower no arquivamento de logs
- Proibir alterações na política dos buckets do S3 criados pelo AWS Control Tower no arquivamento de logs
- Proibir alterações na configuração de ciclo de vida dos buckets do S3 criados pelo AWS Control Tower no arquivamento de logs

A orientação mudou de obrigatória para eletiva:

- Proibir alterações na configuração de criptografia para todos os buckets do Amazon S3 [Anteriormente: Habilitar criptografia em repouso para arquivamento de logs]
- Proibir alterações na configuração de registro em log para todos os buckets do Amazon S3 [Anteriormente: Habilitar o registro em log de acesso para arquivamento de logs]

- Proibir alterações na política de bucket para todos os buckets do Amazon S3 [Anteriormente: Proibir alterações de política no arquivamento de logs]
- Proibir alterações na configuração do ciclo de vida de todos os buckets do Amazon S3 [Anteriormente: Definir uma política de retenção para o arquivamento de logs]

A versão 2.7 do AWS Control Tower inclui alterações no esquema da zona de pouso do AWS Control Tower que podem causar incompatibilidade com versões anteriores após a atualização para 2.7.

- Em particular, a versão 2.7 do AWS Control Tower habilita `BlockPublicAccess` automaticamente em buckets do S3 implantados pelo AWS Control Tower. Você poderá desativar esse padrão se a sua workload exigir acesso em várias contas. Consulte mais informações sobre o que acontece com `BlockPublicaccess` habilitado em Bloquear o acesso público ao armazenamento do Amazon S3.
- A versão 2.7 do AWS Control Tower inclui uma exigência de HTTPS. Todas as solicitações enviadas para buckets do S3 implantados pelo AWS Control Tower devem usar Secure Socket Layer (SSL). Somente solicitações HTTPS são permitidas. Se você usa HTTP (sem SSL) como um endpoint para enviar as solicitações, essa alteração gera um erro de acesso negado, o que pode interromper o fluxo de trabalho. Essa alteração não pode ser revertida após a atualização da zona de pouso para a versão 2.7.

  Recomendamos que você altere suas solicitações para usar TLS em vez de HTTP.

Três novas AWS regiões disponíveis

8 de abril de 2021

(Atualização necessária para a zona de pouso do AWS Control Tower)

O AWS Control Tower está disponível em três AWS regiões adicionais: região Ásia-Pacífico (Tóquio), região Ásia-Pacífico (Seul) e região Ásia-Pacífico (Mumbai). É necessária uma atualização da zona de pouso para a versão 2.7 para expandir a governança nessas regiões.

Sua zona de pouso 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.

Administrar somente regiões selecionadas

19 de fevereiro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

A seleção de região do AWS Control Tower permite gerenciar melhor a área geográfica dos seus recursos do 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 fica disponível quando você configura uma nova zona de pouso ou atualiza a versão da zona de pouso do AWS Control Tower. Quando você usa o Account Factory para criar uma conta ou inscrever uma conta-membro preexistente, ou quando usa Estender governança para inscrever contas em uma unidade organizacional preexistente, o AWS Control Tower implanta seus recursos de governança de registro em log, monitoramento e controles centralizados, nas regiões escolhidas nas contas. Consulte mais informações sobre a seleção de regiões em Configurar regiões do AWS Control Tower.

O AWS Control Tower agora estende a governança às existentes OUs em suas AWS organizações

28 de janeiro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

Estenda a governança às unidades organizacionais (OUs) existentes (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 do AWS Control Tower. Consulte informações sobre como estender a governança a uma UO inteira em Registrar uma unidade organizacional existente com o AWS Control Tower.

Quando você registra uma UO, o AWS Control Tower executa uma série de verificações para garantir a extensão bem-sucedida da governança e a inscrição de contas na UO. Consulte mais informações sobre problemas comuns associados ao registro inicial de uma UO em Causas comuns de falha durante o registro ou 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.

AWS Control Tower disponibiliza atualizações de contas em massa

28 de janeiro de 2021

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

Com o recurso de atualização em massa, agora é possível atualizar com um único clique no painel do AWS Control Tower todas as contas em uma unidade organizacional (UO) registrada do AWS Organizations que contém até 300 contas. Isso é útil principalmente nos casos em que você atualiza a zona de pouso do AWS Control Tower e também deve atualizar as contas inscritas para alinhá-las à versão atual da zona de pouso.

Esse recurso também ajuda a manter suas contas atualizadas quando você atualiza a zona de pouso do AWS Control Tower para expandir a novas regiões, ou quando deseja registrar novamente uma UO a fim de garantir que todas as contas nela 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.

Consulte informações sobre como atualizar uma zona de pouso em Atualizar a zona de pouso.

Consulte informações sobre como registrar ou registrar novamente uma UO em Registrar uma unidade organizacional existente com o AWS Control Tower.

De janeiro a dezembro de 2020

Em 2020, o AWS Control Tower lançou as seguintes atualizações:

- O console do AWS Control Tower agora está vinculado às regras externas do AWS Config
- AWS Control Tower já disponível em mais regiões
- Atualização da barreira de proteção
- O console do AWS Control Tower mostra mais detalhes sobre contas OUs e
- Use o AWS Control Tower para configurar novos AWS ambientes de várias contas em AWS Organizations
- Solução Customizations for AWS Control Tower
- Disponibilidade geral do AWS Control Tower versão 2.3
- Provisionamento de contas em uma única etapa no AWS Control Tower

- Ferramenta de desativação do AWS Control Tower
- Notificações de eventos de ciclo de vida do AWS Control Tower

O console do AWS Control Tower agora está vinculado às regras externas do AWS Config

29 de dezembro de 2020

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 2.6. Consulte informações em Atualizar a zona de pouso)

O AWS Control Tower agora inclui um agregador em nível organizacional, que ajuda na detecção de regras externas do Config. AWS Isso fornece visibilidade no console do AWS Control Tower para ver a existência de regras de AWS configuração criadas externamente, além das regras de AWS configuração criadas pela AWS Control Tower. O agregador permite que o AWS Control Tower detecte regras externas e forneça um link para o console AWS Config sem a necessidade de o AWS Control Tower obter acesso a contas não gerenciadas.

Com esse recurso, agora você tem uma visão consolidada dos controles de detecção aplicados às suas contas para poder monitorar a conformidade e determinar se precisa de controles adicionais para sua conta. Para obter informações, consulte Como o AWS Control Tower agrega AWS Config regras em contas OUs e não gerenciadas.

AWS Control Tower já disponível em mais regiões

18 de novembro de 2020

(É necessário atualizar a zona de pouso do AWS Control Tower para a versão 2.5. Consulte informações em Atualizar a zona de pouso)

O AWS 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 dessas 5 AWS regiões é a única alteração introduzida para a versão 2.5 do AWS Control Tower.

O AWS Control Tower também está disponível nas regiões Leste dos EUA (N. da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Europa (Irlanda) e Ásia-Pacífico (Sydney). Com esse lançamento, o AWS Control Tower agora está disponível em 10 AWS regiões.

Essa atualização da zona de pouso 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 no AWS Control Tower para governar as 10 regiões suportadas AWS . Para mais informações, consulte Configurar regiões do AWS Control Tower.

Atualização da barreira de proteção

8 de outubro de 2020

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

Uma versão atualizada foi lançada para o controle obrigatório `AWS-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 o perfil `AWSControlTowerExecution` habilitado. A versão anterior do controle impede que esse perfil seja criado.

Para obter mais informações, consulte Não permitir alterações nas funções AWS do IAM configuradas pelo AWS Control Tower e AWS CloudFormation no Guia de referência de controles do AWS Control Tower.

O console do AWS Control Tower mostra mais detalhes sobre contas OUs e

22 de julho de 2020

(Não é necessário atualizar a zona de pouso do 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 suas AWS contas e unidades organizacionais (OUs). A página Contas agora lista todas as contas da organização,

independentemente da UO ou do status de inscrição no AWS Control Tower. Agora é possível pesquisar, classificar e filtrar em todas as tabelas.

Use o AWS Control Tower para configurar novos AWS ambientes de várias contas em AWS Organizations

22 de abril de 2020

(Não é necessário atualizar a zona de pouso do 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:

- AWS Organizations Os clientes existentes agora podem configurar um novo 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 a 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.

O AWS 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 seu AWS ambiente de várias contas novo ou existente e governar em grande escala. Com uma organização administrada pelo 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 novas AWS contas rapidamente, sem preocupações indevidas com a conformidade.

Consulte informações sobre como configurar uma zona de pouso em Planejar a zona de pouso do 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 Inscrever conta. Agora, permite a inscrição de AWS contas existentes, bem como a criação de novas contas. Para obter mais informações, consulte Inscrever uma conta existente.

Solução Customizations for AWS Control Tower

17 de março de 2020

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora inclui uma nova implementação de referência que facilita a aplicação de modelos e políticas personalizados à sua zona de pouso do 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 personalizadas de controle de serviços (SCPs) a essas contas, além das SCPs já fornecidas pelo AWS Control Tower. O pipeline do Customizations for AWS Control Tower se integra aos eventos e notificações do ciclo de vida do AWS Control Tower (Eventos de ciclo de vida no AWS Control Tower) para garantir que as implantações de recursos permaneçam sincronizadas com a zona de pouso.

A documentação de implantação dessa arquitetura de solução do AWS Control Tower está disponível no site de soluções da AWS.

Disponibilidade geral do AWS Control Tower versão 2.3

5 de março de 2020

(Atualização necessária para a zona de pouso do AWS Control Tower. Consulte informações em Atualizar a zona de pouso.)

O AWS Control Tower agora está disponível na AWS região Ásia-Pacífico (Sydney), 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 ainda não usou o AWS Control Tower, pode iniciá-lo hoje em qualquer uma das regiões compatíveis. Se você já estiver usando o 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 do AWS Control Tower. Nessa página, atualize a zona de pouso para a versão mais recente. Depois, atualize suas contas individualmente.

> **Note**
>
> Atualizar a zona de pouso não atualiza automaticamente as contas. Se você tiver mais do que algumas contas, as atualizações necessárias podem ser demoradas. Por esse motivo, recomendamos que você evite expandir a zona de pouso do AWS Control Tower para regiões nas quais as workloads não precisam ser executadas.

Consulte informações sobre o comportamento esperado dos controles de detecção como resultado de uma implantação em uma nova região em Configure your AWS Control Tower Regions.

Provisionamento de contas em uma única etapa no AWS Control Tower

2 de março de 2020

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora é compatível com o provisionamento de contas em uma única etapa por meio do console do AWS Control Tower. Esse recurso permite provisionar novas contas de dentro do console do AWS Control Tower.

Para usar o formulário simplificado, acesse o Account Factory no console do AWS Control Tower e escolha Provisionamento rápido de contas. O AWS Control Tower atribui o mesmo endereço de e-mail à conta provisionada e ao usuário de login único (Centro de Identidade do IAM) criado para a conta. Se for necessário 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 AWS Service Catalog o Account Factory do AWS Control Tower, exatamente como você atualizaria 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 do AWS Control Tower foi separada da capacidade de cadastrar AWS contas. Para obter mais informações, consulte Inscrever uma conta existente.

Ferramenta de desativação do AWS Control Tower

28 de fevereiro de 2020

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora é compatível com uma ferramenta automatizada de desativação para ajudar você a limpar os recursos alocados pelo AWS Control Tower. Caso não pretenda mais usar o AWS Control Tower para sua empresa, ou ainda, caso precise de uma grande reimplantação de

recursos organizacionais, talvez você queira limpar os recursos criados na configuração inicial da sua zona de pouso.

Para descomissionar sua landing zone usando um processo que é basicamente automatizado, entre em contato AWS Support para obter ajuda com as etapas adicionais necessárias. Consulte mais informações sobre a desativação em Descomissione uma landing zone do AWS Control Tower.

Notificações de eventos de ciclo de vida do AWS Control Tower

22 de janeiro de 2020

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower anuncia a disponibilidade de notificações de eventos de 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.

O AWS Control Tower registra eventos de ciclo de vida após a conclusão das seguintes ações que podem ser realizadas usando o serviço: criar ou atualizar uma zona de pouso; criar ou excluir uma UO; habilitar ou desabilitar um controle em uma UO; e usar o Account Factory para criar um conta ou mover uma conta para outra UO.

O AWS Control Tower usa vários AWS serviços para criar e administrar um ambiente multicontas AWS de melhores práticas. Pode levar vários minutos para que uma ação do AWS Control Tower seja concluída. Você pode rastrear eventos do ciclo de vida nos CloudTrail registros para verificar se a ação original do AWS Control Tower foi concluída com sucesso. 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.

De janeiro a dezembro de 2019

De 1.º de janeiro a 31 de dezembro de 2019, o AWS Control Tower lançou as seguintes atualizações:

- Disponibilidade geral do AWS Control Tower versão 2.2
- Novos controles eletivos no AWS Control Tower
- Novos controles de detecção no AWS Control Tower

- AWS 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 zona de pouso do AWS Control Tower. Consulte informações em Atualizar a zona de pouso.)

A versão 2.2 do AWS Control Tower fornece três novos controles preventivos que evitam desvios nas contas:

- Proibir alterações nos grupos de log do Amazon CloudWatch Logs configurados pelo AWS Control Tower
- Proibir a exclusão de autorizações de AWS Config agregação criadas pelo AWS Control Tower
- Proibir a exclusão do arquivamento de logs

Um controle é uma regra de alto nível que fornece governança contínua para todo o ambiente da AWS . Quando você cria sua zona de pouso do 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. À medida que você e os membros da organização usam a zona de pouso, podem ocorrer alterações (acidentais ou intencionais) no status de conformidade. 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 Detectar e resolver desvios no AWS Control Tower.

Novos controles eletivos no AWS Control Tower

5 de setembro de 2019

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora inclui estes quatro novos controles eletivos:

- Proibir a exclusão de ações em buckets do Amazon S3 sem MFA
- Proibir alterações na configuração de replicação para buckets do Amazon S3

- Proibir ações como usuário-raiz
- Proibir a criação de chaves de acesso para o usuário-raiz

Um controle é uma regra de alto nível que fornece governança contínua para todo o ambiente da AWS . As proteções permitem que você expresse suas intenções políticas. Consulte mais informações em About controls in AWS Control Tower.

Novos controles de detecção no AWS Control Tower

25 de agosto de 2019

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

O AWS Control Tower agora inclui estes oito novos controles de detecção:

- Detectar se o versionamento para buckets do Amazon S3 está habilitado
- Detecte se o MFA está habilitado para usuários IAM do console AWS
- Detectar se a MFA está habilitada para usuários do IAM
- Detecte se a otimização do Amazon EBS está habilitada para instâncias da Amazon EC2
- Detecte se os volumes do Amazon EBS estão conectados às instâncias da Amazon EC2
- Detectar se o acesso público às instâncias de banco de dados do Amazon RDS está habilitado
- Detectar se o acesso público aos snapshots de banco de dados do Amazon RDS está habilitado
- Detectar se a criptografia de armazenamento está habilitada para instâncias de banco de dados do Amazon RDS

Um controle é uma regra de alto nível que fornece governança contínua para todo o ambiente da AWS . Um controle de detecção detecta a não conformidade de recursos em suas contas, como violações de políticas, e fornece alertas por meio do painel. Consulte mais informações em About controls in AWS Control Tower.

AWS Control Tower aceita endereços de e-mail para contas compartilhadas com domínios diferentes da conta de gerenciamento

1.º de agosto de 2019

(Não é necessário atualizar a zona de pouso do AWS Control Tower)

No AWS Control Tower, agora é possível enviar endereços de e-mail para contas compartilhadas (arquivamento de logs e membro de auditoria) e contas secundárias (fornecidas usando o Account Factory) cujos domínios são diferentes do endereço de e-mail da conta de gerenciamento. Esse recurso fica disponível somente quando você cria uma zona de pouso e quando você provisiona novas contas secundárias.

Disponibilidade geral do AWS Control Tower versão 2.1

24 de junho de 2019

(Atualização necessária da zona de pouso do AWS Control Tower. Consulte informações em Update Your Landing Zone.)

O AWS Control Tower já está disponível para o público e é compatível para uso na produção. O AWS Control Tower é destinado a organizações com várias contas e equipes que buscam a maneira mais fácil de configurar seu novo AWS ambiente de várias contas e governar em grande escala. Com o AWS Control Tower, você pode ajudar a garantir que as contas da sua organização estejam em conformidade com as políticas estabelecidas. Os usuários finais em equipes distribuídas podem provisionar novas AWS contas rapidamente.

Usando o AWS Control Tower, você pode configurar uma landing zone que emprega as melhores práticas, como configurar uma estrutura de várias contas usando AWS Organizations, gerenciar identidades de usuários e acesso federado com AWS IAM Identity Center, habilitar o provisionamento de contas por meio do Service Catalog e criar um arquivo de log centralizado usando e. AWS CloudTrail AWS Config

Para uma governança contínua, é possível habilitar controles pré-configurados, que são regras claramente definidas para segurança, operações e conformidade. As barreiras 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 habilitados e o status de conformidade das contas.

É possível configurar um novo ambiente de várias contas com um único clique no console do AWS Control Tower. Não há cobranças adicionais nem compromissos antecipados para usar o AWS Control Tower. Você paga somente pelos AWS serviços que habilitou para configurar uma landing zone e implementar os controles selecionados.

Histórico do documento

- Última atualização da documentação: 10 de dezembro de 2024

A tabela a seguir descreve as alterações importantes feitas no Guia do usuário do AWS Control Tower. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
O AWS Control Tower atualiza uma função vinculada ao serviço	Atualizações para `AWSControlTowerAccountServiceRolePolicy` .	10 de dezembro de 2024
O AWS Control Tower cFct suporta GitHub	Uma nova opção para uma fonte de configuração de terceiros.	9 de dezembro de 2024
Controles preventivos do AWS Control Tower com políticas declarativas	Um novo tipo de política implementa um novo tipo de controle preventivo.	1.º de dezembro de 2024
O AWS Control Tower se integra ao Backup AWS	Você pode configurar planos para fazer backup dos seus recursos do AWS Control Tower.	25 de novembro de 2024
O AWS Control Tower integra AWS Config controles	O AWS Control Tower integra AWS Config controles selecionados.	21 de novembro de 2024
O AWS Control Tower melhora o gerenciamento de ganchos	O AWS Control Tower agora gerencia ganchos para controles proativos.	20 de novembro de 2024
Desvio da política de controle relatado	O AWS Control Tower relata um novo tipo de desvio.	15 de novembro de 2024

AWS Control Tower lança políticas gerenciadas de controle de recursos	Um novo tipo de controle preventivo, implementado com RCPs.	15 de novembro de 2024
AWS Control Tower adiciona ResetEnabledControl API	Uma nova API para gerenciar o desvio de controle.	14 de novembro de 2024
`GetControl` API atualizada	Dois novos campos de controle para`GetControl` .	8 de novembro de 2024
AFT do AWS Control Tower é compatível com o GitLab	Uma nova opção para uma fonte de configuração de terceiros.	23 de outubro de 2024
O AWS Control Tower está disponível na região AWS Ásia-Pacífico (Malásia)	Uma nova região está disponível, Malásia (Kuala Lumpur).	21 de outubro de 2024
AWS Control Tower é compatível com até mil contas por UO	Um aumento do limite de contas por UO.	30 de agosto de 2024
AWS Control Tower adiciona a seleção de versão da zona de pouso	Atualize ou repare a zona de pouso sem mudar para a versão mais recente, se você estiver executando a versão 3.1 ou posterior.	15 de agosto de 2024
GetControl e operações de ListControls API disponíveis	Duas novas operações do Catálogo de controles ajudam a encontrar mais informações sobre os controles.	6 de agosto de 2024
AWS Control Tower é compatível com AFT e CfCT em regiões opcionais	AFT e CFct estão disponíve is adicionalmente Regiões da AWS.	18 de julho de 2024

AWS Control Tower adiciona a API `ListLandingZoneOperations`	Uma nova API que permite que você recupere operações recentes para a zona de pouso.	26 de junho de 2024
AWS Control Tower permite até 100 operações de controle simultâneas	Um aumento da cota de operações de controle simultâneas para 100.	20 de maio de 2024
O AWS Control Tower está disponível na região Oeste de AWS Calgary (Canadá)	O AWS Control Tower está disponível na região Oeste do Canadá (Calgary).	3 de maio de 2024
AWS Control Tower permite ajustes na cota de autoatendimento	O AWS Control Tower é integrado às AWS Service Quotas no console.	25 de abril de 2024
A documentação dos controles foi movida para um novo guia	AWS Control Tower publica o Guia de referência de controles.	21 de abril de 2024
Marcar recursos `EnabledControl` no AWS CloudFormation	O AWS Control Tower oferece suporte à adição de tags aos `EnabledControl` recursos por meio de AWS CloudFormation modelos.	22 de fevereiro de 2024
Linha de base disponível APIs	O AWS Control Tower lançou uma novidade APIs para registro OUs programático.	14 de fevereiro de 2024
Versão 3.3 da zona de pouso do AWS Control Tower	Versão 3.3 da zona de pouso do AWS Control Tower disponível.	14 de dezembro de 2023

AWS Control Tower anuncia controles para auxiliar a soberania digital	AWS Control Tower lançou um grupo de controles para ajudar os clientes com os requisitos de soberania digital.	27 de novembro de 2023
O AWS Control Tower é compatível com landing zone APIs	O AWS Control Tower oferece suporte à configuração e ao lançamento de zonas de pouso usando novas APIs.	26 de novembro de 2023
AWS Control Tower permite marcar controles habilitados	O AWS Control Tower oferece suporte à marcação de controles habilitados, no console e com novos APIs.	10 de novembro de 2023
AWS Control Tower disponível na Ásia-Pacífico (Melbourne) Região da AWS	Disponível na região Ásia-Pacífico (Melbourne).	3 de novembro de 2023
Nova API de controle disponível	O AWS Control Tower adicionou uma nova API de controle.	14 de outubro de 2023
AWS Control Tower lança novos controles	O AWS Control Tower lançou novos controles proativos e de detecção.	5 de outubro de 2023
AWS Control Tower relata desvio da desabilitação de acesso confiável	O AWS Control Tower notificará os clientes quando ocorre um desvio, se os clientes desativarem o acesso confiável ao AWS Control Tower no AWS Organizations.	21 de setembro de 2023
O AWS Control Tower está disponível em mais quatro Regiões da AWS	Disponível nas regiões Ásia-Pacífico (Hyderabad), Europa (Espanha e Zurique) e Oriente Médio (EAU).	13 de setembro de 2023

AWS Control Tower disponível na região Tel Aviv	O AWS Control Tower anuncia disponibilidade na região Tel Aviv, il-central-1.	28 de agosto de 2023
AWS Control Tower lança 28 novos controles proativos	O AWS Control Tower lançou 28 novos controles proativos.	24 de julho de 2023
AWS Control Tower desativa dois controles	O AWS Control Tower removerá dois controles da biblioteca de controles, a partir de 18 de agosto de 2023.	18 de julho de 2023
Zona de pouso 3.2 do AWS Control Tower disponível	A versão 3.2 da zona de pouso do AWS Control Tower já está disponível.	16 de junho de 2023
AWS Control Tower gerencia contas com base em ID	O AWS Control Tower rastreia o ID da AWS conta, em vez do endereço de e-mail da conta.	14 de junho de 2023
Controles de detecção adicionais do Security Hub disponíveis	O AWS Control Tower adiciona dez novos controles à biblioteca de controles do padrão de gerenciado pelo serviço Security Hub: AWS Control Tower.	12 de junho de 2023
AWS Control Tower publica tabelas de metadados de controle	O AWS Control Tower agora fornece tabelas de metadados de controle como parte da documentação publicada.	7 de junho de 2023
Suporte do Terraform para o Account Factory Customization	Suporte de região única para esquemas de código aberto do Terraform no AFC.	6 de junho de 2023

AWS Autogerenciamento do IAM disponível para landing zone	O AWS Control Tower agora ajuda os clientes a escolher seu provedor de identidade para uma zona de pouso.	6 de junho de 2023
Novo perfil adicionado	O AWS Control Tower adicionou uma nova função vinculada ao serviço, AWSServiceRoleForAWSControlTorre, e política associada,. AWSControlTowerAccountServiceRolePolicy	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 a administrar seu ambiente de várias contas e a atingir objetivos específicos de controle.	19 de maio de 2023
Sete regiões adicionais disponíveis	O AWS 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

Alteração para uma política gerenciada	Alteramos o AWSControlTowerServiceRolePolicypara que o AWS Control Tower possa chamar os`EnableRegion` ,`ListRegions` , `GetRegionOptStatus` APIs que são implementados pelo serviço de gerenciamento de AWS contas.	6 de abril de 2023
Rastreamento de solicitações de personalização de conta disponível para o público	O AWS Control Tower agora permite rastrear solicitações de personalização de contas usando o fluxo de trabalho Account Factory for Terraform (AFT).	16 de fevereiro de 2023
Atualização de práticas recomendadas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	15 de fevereiro de 2023
Zona de pouso 3.1 do AWS Control Tower disponível	A zona de pouso 3.1 do AWS Control Tower está disponível.	9 de fevereiro de 2023
Controles proativos disponíveis ao público	Os controles proativos são iniciados desde o status de pré-visualização até a disponibilidade para o público.	24 de janeiro de 2023

Operações de conta simultâneas	O AWS Control Tower agora permite até cinco (5) ações simultâneas no Account Factory. É possível criar, atualizar ou inscrever até cinco contas por vez.	16 de dezembro de 2022
Controles proativos auxiliam no provisionamento de recursos	O AWS Control Tower agora oferece suporte a controles proativos, implementados por meio de AWS CloudFormation ganchos.	28 de novembro de 2022
Personalização do Account Factory disponível	O AWS Control Tower agora permite o provisionamento de contas com modelos de conta personalizáveis, chamados de esquemas, diretamente do console do AWS Control Tower.	28 de novembro de 2022
Status de conformidade visível para todas as AWS Config regras	O AWS Control Tower agora exibe o status de conformidade de todas as AWS Config regras implantadas em unidades organizacionais registradas na AWS Control Tower.	18 de novembro de 2022
Alteração para uma política gerenciada	Alteramos o AWSControlTowerServiceRolePolicypara que o AWS Control Tower possa assumir a `AWSControlTowerBlueprintAccess` função, que é necessária para as personalizações do Account Factory.	28 de outubro de 2022

APIs para controles, AWS CloudFormation recursos	O AWS Control Tower agora oferece suporte à ativação e desativação de controles por meio de um conjunto de chamadas de API e de um novo AWS CloudFormation recurso.	1.º de setembro de 2022
O CfCT permite a exclusão do conjunto de pilhas	O CfCT permite a exclusão do conjunto de pilhas, definindo um parâmetro no arquivo de manifesto.	26 de agosto de 2022
Retenção de logs personalizada	Você pode personalizar a política de retenção para buckets Amazon S3 que armazenam seus CloudTrail 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 perfil disponível	O AWS Control Tower permite reparar desvios de perfil, sem um reparo completo da zona de pouso.	11 de agosto de 2022

Versão 3.0 disponível	A versão 3.0 da zona de pouso do AWS Control Tower muda de AWS CloudTrail trilhas baseadas em contas para trilhas baseadas em 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 de região e dois novos controles de detecção.	29 de julho de 2022
A página Organização combina visualizações OUs e contas	A nova página da organização no AWS Control Tower mostra uma visão hierárquica de todas as unidades organizac ionais (OUs) e contas.	18 de julho de 2022
Alteração para uma política gerenciada	Alteramos o AWSContro lTowerServiceRolePolicypara que os clientes possam ter AWS CloudTrail trilhas em nível organizacional para agregar registros. AWS CloudTrail	20 de junho de 2022

Inscrição e atualização mais fáceis para contas-membros	O AWS Control Tower agora permite cadastrar e atualizar contas-membros individua lmente, de dentro da zona de pouso. 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
AFT permite personalização de contas compartilhadas	O Account Factory for Terraform do AWS Control Tower agora permite personali zar a conta de gerenciamento, a conta de auditoria e a conta de arquivamento de logs do AWS Control Tower.	27 de maio de 2022
Operações simultâneas para todos os controles opcionais	Agora, o AWS Control Tower permite aplicar e remover barreiras de proteção preventivas opcionais simultaneamente, bem como controles de detecção.	18 de maio de 2022
Contas de segurança e de registro em log existentes	O AWS Control Tower agora permite trazer contas de segurança e registro em log existentes, em vez de criar outras durante a configuração da zona de pouso.	16 de maio de 2022

Versão 2.9 disponível	A versão 2.9 da zona de pouso do AWS Control Tower atualiza o encaminhador de notificações do Lambda para usar o runtime do Python versão 3.9.	22 de abril de 2022
Suporte atualizado para as AWS melhores práticas, versão 2.8 disponível	A versão 2.8 da zona de pouso do AWS Control Tower fornece suporte adicional para garantir que suas cargas de trabalho e AWS contas estejam alinhadas com as AWS melhores práticas.	10 de fevereiro de 2022
Controle de negação de região	O AWS Control Tower agora inclui um controle que ajuda você a restringir o acesso às AWS regiões para lidar com questões regulatórias e de conformidade.	30 de novembro de 2021
Controles de residência de dados	O AWS Control Tower agora é compatível com controles que ajudam a gerenciar a residência de dados com controle granular.	30 de novembro de 2021
Account Factory for Terraform do AWS Control Tower	O AWS Control Tower agora é compatível com o Terraform para provisionamento e atualização automáticos de contas.	29 de novembro de 2021

Novo evento do ciclo de vida disponível	O `PrecheckOrganizationalUnit` evento registra se algum recurso impede o sucesso da tarefa de governança Extend, incluindo recursos aninhados OUs.	18 de novembro de 2021
Aninhado disponível OUs	O AWS Control Tower agora permite que a zona de pouso contenha estruturas de UO aninhadas.	16 de novembro de 2021
Simultaneidade do controle de detecção	Os controles de detecção do AWS Control Tower agora permitem operações simultâneas de habilitação e desabilitação.	5 de novembro de 2021
Duas novas regiões disponíveis	O AWS Control Tower agora está disponível em duas novas AWS regiões, a região da Europa (Paris) e a região da América do Sul (São Paulo).	29 de julho de 2021
Desmarcação de região	Você pode desmarcar AWS regiões que não deseja mais governar por meio do AWS Control Tower.	29 de julho de 2021
Chaves do KMS disponíveis	Opcionalmente, você pode criar ou escolher as chaves do KMS que gerencia para criptografar seus dados e recursos.	28 de julho de 2021

Alteração para uma política gerenciada	Alteramos o AWSControlTowerServiceRolePolicypara que os clientes possam usar suas próprias chaves de criptografia KMS para AWS CloudTrail registros.	28 de julho de 2021
Nomes de controle alterados, funcionalidade inalterada	Alguns nomes e descrições de controle foram atualizados para refletir melhor as intenções políticas do controle, sem alteração na funcionalidade.	26 de julho de 2021
Escaneamentos automatizados de arquivos gerenciados SCPs	O AWS Control Tower realiza escaneamentos automatizados diários de arquivos gerenciados SCPs para verificar se há desvio.	11 de maio de 2021
Nomes OUs e contas personalizados	O AWS 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

Desativar uma zona de pouso por autoatendimento	Agora, o AWS Control Tower permite desativar uma zona de pouso sem entrar em contato com o AWS Support. A desativação é um processo semiautomático 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	O AWS Control Tower agora está disponível em três AWS regiões adicionais: região Ásia-Pacífico (Tóquio), região Ásia-Pacífico (Seul) e região Ásia-Pacífico (Mumbai).	8 de abril de 2021
Novos controles de arquivamento de logs, versão 2.7 da zona de pouso disponível	Quatro novos controles de arquivamento de logs fornecem governança de arquivamento de logs sobre os recursos do AWS Control Tower, separadamente da governança de recursos fora do AWS Control Tower. A orientação sobre os quatro controles existentes mudou de obrigatória para eletiva. A versão 2.7 da zona de pouso do AWS Control Tower inclui um requisito de HTTPS, que não pode ser desfeito após a atualização.	8 de abril de 2021

Seleção da região	A seleção de região do AWS Control Tower permite gerenciar melhor a área geográfica dos seus recursos do AWS Control Tower. Para expandir o número de regiões nas quais você hospeda recursos ou workloads da AWS , por motivos de conformidade, regulamentação, custo ou outros, agora você pode selecionar as regiões adicionais a administrar.	19 de fevereiro de 2021
Registrar uma UO e controle todas as suas contas com o AWS Control Tower de uma só vez	O AWS Control Tower permite registrar uma UO, 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 unidade AWS Organizations organizacional (OU) registrada contendo até 300 contas, com um único clique, no painel do AWS Control Tower. O recurso de atualização de várias contas, também conhecido como atualização 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 gerenciadas OUs	Uma nova função ajuda na detecção de AWS Config regras externas, para que o AWS Control Tower não precise obter acesso a contas não gerenciadas.	29 de dezembro de 2020

O AWS Control Tower está disponível em mais AWS regiões.	O AWS Control Tower já está disponível para implantação nas regiões Ásia-Pacífico (Singapura), Europa (Frankfurt), Europa (Londres), Europa (Estocolmo), Canadá (Central). Com esse lançamento, o AWS Control Tower agora está disponível em 10 AWS regiões. Essa atualização da zona de pouso 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 no AWS Control Tower para governar as 10 regiões suportadas AWS .	18 de novembro de 2020
Atualização de controle	Uma versão atualizada foi lançada para o controle obrigatório `AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` . O controle atualizado viabiliza uma inscrição automática de contas mais fácil.	8 de outubro de 2020
Página de informações relacionadas já está disponível para o AWS Control Tower	A página de informações relacionadas facilita a localização de tarefas comuns que podem ser úteis após a configuração da zona de pouso do AWS Control Tower.	18 de setembro de 2020

O console do AWS Control Tower mostra mais detalhes sobre contas OUs e contas.	No console do AWS Control Tower, você pode ver mais detalhes sobre suas AWS contas e unidades organizacionais (OUs). A página “Contas” agora lista todas as contas da organização, independentemente da UO ou do status de inscrição no AWS Control Tower. Agora é possível pesquisar, classificar e filtrar em todas as tabelas.	22 de julho de 2020
AWS Control Tower permite que as organizações existentes configurem uma zona de pouso	Agora, é possível iniciar uma zona de pouso para o AWS Control Tower em uma organização existente, para incluir 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 AWS contas existentes, bem como a criação de novas contas.	16 de abril de 2020
AWS Control Tower já disponível na região Ásia-Pacífico	O AWS Control Tower agora está disponível para ser implantado na AWS região Ásia-Pacífico (Sydney). Essa versão requer atualizações manuais para contas fornecidas. Atualize apenas se planeja executar workloads na região Ásia-Pacífico (Sydney).	3 de março de 2020

A desativação de uma zona de pouso do AWS Control Tower é possível	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
Provisionamento rápido de contas está disponível no AWS Control Tower	O provisionamento rápido de contas facilita a execução de novas contas-membros quando a zona de pouso está atualizada, com o recurso Inscrever conta.	20 de fevereiro de 2020
Eventos de ciclo de vida são monitorados no AWS Control Tower	Os eventos de ciclo de vida fornecem detalhes adicionais para determinados eventos do AWS Control Tower, para facilitar a automação do fluxo de trabalho.	12 de dezembro de 2019
As páginas Configurações e Atividades estão disponíveis para o 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 o 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 detecção adicionais estão disponíveis para o AWS Control Tower	Os controles de detecção no AWS Control Tower fornecem informações sobre o estado de sua organização e seus recursos.	27 de agosto de 2019
AWS Control Tower já está disponível ao público	O AWS Control Tower é um serviço que oferece a maneira mais fácil de configurar e governar seu AWS ambiente de várias contas em grande escala.	24 de junho de 2019

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário 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.