Estrutura de OU em zonas de AWS pouso regulamentadas: um exemplo da indústria farmacêutica

AWS Recomendações

AWS Recomendações: Estrutura de OU em zonas de AWS pouso regulamentadas: um exemplo da indústria farmacêutica

Table of Contents

Estrutura de OU em zonas de AWS pouso regulamentadas: um exemplo da indústria farmacêutica

Katja Mueller, Petar Forai e Keval Sheth, Amazon Web Services (AWS)

Março de 2023 (histórico do documento)

AWS fornece várias configurações do Landing Zone Accelerator que oferecem suporte a setores específicos, incluindo saúde. O Landing Zone Accelerator for Healthcare é usado em conjunto AWS Control Tower para facilitar o gerenciamento e a governança de um ambiente de várias contas que está alinhado às AWS melhores práticas e a várias estruturas globais de conformidade. Um aspecto importante da orquestração da governança é Contas da AWS agrupar usando unidades organizacionais (OUs), para que você possa administrá-las como uma única unidade.

Este guia analisa as práticas recomendadas e considerações para redesenhar as estruturas de UO existentes à medida que a maturidade da nuvem da sua empresa cresce. Ele apresenta um exemplo prático baseado na AWS Control Tower implementação de uma grande empresa farmacêutica e discute as lições aprendidas com essa implementação. AWS o design da landing zone não é um esforço único. Ela pode e deve evoluir. Essa evolução pode ser alcançada com sucesso e eficiência aplicando as AWS melhores práticas e dicas destacadas neste guia.

Visão geral

Trabalhamos com uma empresa farmacêutica multinacional para realizar atividades de prova de conceito (PoC) na AWS a fim de analisar como ela poderia migrar suas aplicações on-premises para a Nuvem AWS. Quando começaram a escalar e acelerar seu fluxo de trabalho de migração para incluir workloads de produção, ficou claro que precisavam de uma zona de pouso da AWS regulamentada e compatível para apoiar sua meta. Usamos o AWS Control Tower para projetar e implementar uma nova zona de pouso da AWS.

Um aspecto importante de uma nova zona de pouso da AWS e de sua organização é a estrutura de suas unidades organizacionais (UOs). Uma UO é um agrupamento lógico de Contas da AWS criadas usando o AWS Organizations. Você pode usar UOs para organizar as Contas da AWS em uma hierarquia e aplicar controles de gerenciamento e governança de forma consistente e mais fácil.

Você pode anexar controles baseados em políticas a uma UO e a Contas da AWS. As UOs secundárias em uma UO herdam automaticamente esses controles. Portanto, as UOs desempenham um papel fundamental no gerenciamento da segurança e da governança no AWS Organizations.

Uma política é um documento JSON que inclui uma ou mais instruções que definem os controles que você deseja aplicar a um grupo de Contas da AWS. O AWS Organizationsatualmente é compatível com quatro tipos de políticas, também conhecidas como políticas de controle de serviços (SCPs). Um SCP define as ações e os Serviços da AWS que estão disponíveis para uso em diferentes Contas da AWS. Por exemplo, você pode usar uma SCP para exigir que a instância do Amazon Elastic Compute Cloud (Amazon EC2) seja inicializada com um tipo de instância específico.

Tipos de políticas

Os tipos de política SCP incluem o seguinte:

- Listas de permissões e listas de negações são estratégias complementares que você pode usar para aplicar SCPs para filtrar as permissões disponíveis para as contas.
- As políticas de marcação ajudam você a manter tags consistentes, incluindo o tratamento preferencial de maiúsculas e minúsculas de chaves e os valores das tags nas contas.
- As políticas de backup configuram os backups para os tipos de recursos compatíveis, como a janela de tempo do backup e os cofres de destino para backups nas Regiões da AWS.
- As políticas de exclusão de serviços de IA possibilitam ou não a melhoria contínua dos serviços de inteligência artificial da AWS em todo o mundo.

Política de comportamento herdado: quando você anexa uma política a uma UO específica, as contas que estão diretamente sob essa UO ou qualquer UO secundária herdam a política. Quando você anexa uma política a uma conta específica, ela afeta apenas essa conta. Você pode substituir políticas herdadas introduzindo políticas de exceção. A herança permite explicitamente que todas as permissões fluam da raiz (UO) para cada Conta da AWS nessa UO e na UO secundária, a menos que você negue explicitamente uma permissão. Para negar uma permissão, você cria uma política adicional e a anexa à UO apropriada ou à Conta da AWS. Para obter mais informações sobre exceções e herança de políticas, consulte a documentação do AWS Organizations.

O AWS Control Tower também fornece seu próprio conjunto de controles preventivos e de detecção (também chamados de barreiras de proteção) usando a estrutura da UO. Os controles preventivos do AWS Control Tower evitam ações usando os SCPs no AWS Organizations. Controles de detecção reportam sobre o desvio configuracional em relação ao controle usando o AWS Config. Para obter mais informações sobre esses controles, consulte a documentação do AWS Control Tower.

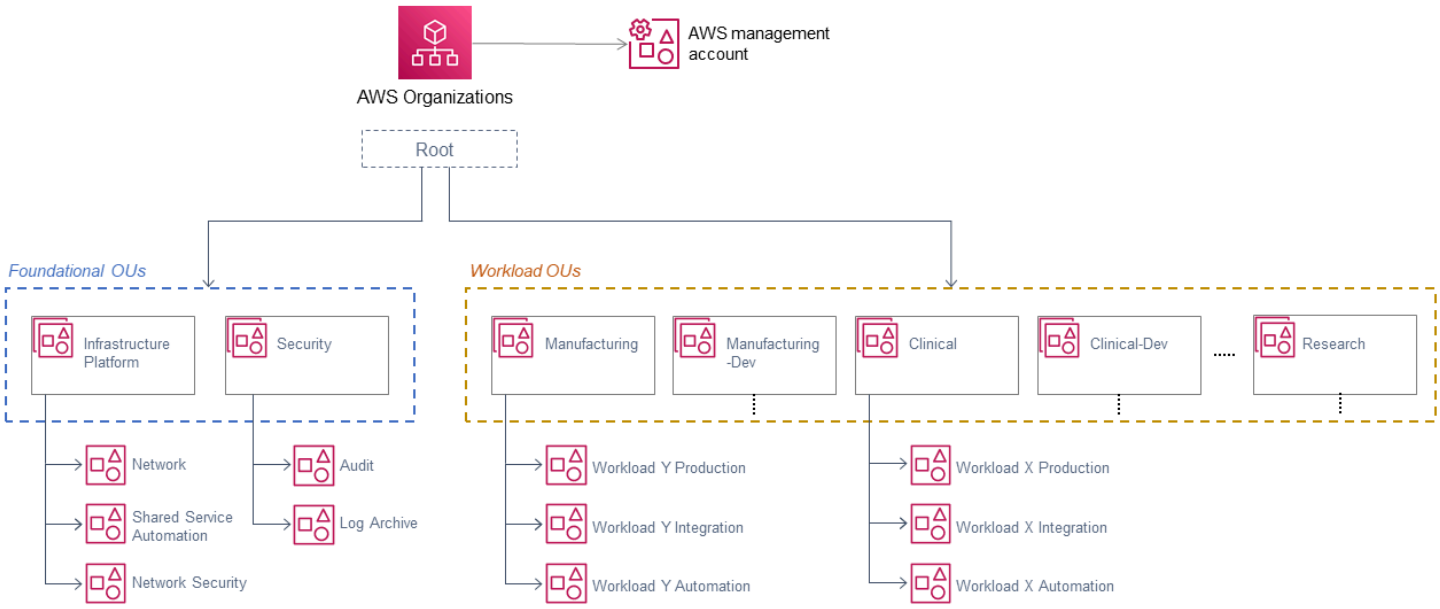
Você também pode habilitar o AWS Security Hub CSPM para automatizar as verificações de práticas recomendadas de segurança, agregar alertas de segurança em um único local e formato e entender a postura geral de segurança em todas as suas Contas da AWS.

Design de UO: fase 1

Para a empresa farmacêutica multinacional em nosso exemplo, o design inicial das organizações e OUs seguiu de AWS Organizations perto AWS as recomendações de configuração AWS Control Tower. Para ver um exemplo, consulte o Landing Zone Accelerator on AWS for Healthcare. AWS Control Tower inicialmente provisionou uma estrutura de OU simples com OUs fundamentais comuns, conforme descrito na postagem do blog Melhores práticas para unidades organizacionais com AWS Organizations, incluindo a OU de segurança, a OU de infraestrutura de plataforma e OUs específicas da empresa.

Design da arquitetura

O diagrama a seguir mostra a arquitetura inicial da UO.



UO de segurança

A OU de segurança agrupa amplamente os Contas da AWS relacionados à funcionalidade de segurança e usa duas contas (auditoria e arquivamento de registros) para armazenar dados operacionais de segurança para acesso central de registros e auditoria ao ambiente. AWS os principais serviços de segurança, como a Amazon GuardDuty , AWS Security Hub CSPM residem na conta de auditoria.

UO de plataforma de infraestrutura

A Plataforma de Infraestrutura OU agrupa Contas da AWS os grupos que fornecem a base da infraestrutura. Inicialmente implantados nessa OU estão os componentes Contas da AWS de rede central (gateways, firewalls, hub de rede central e serviços similares).

UOs adicionais

Outras UOs específicas da empresa (como uma UO clínica) aumentam as UOs fundamentais dentro de uma hierarquia de nível baixo. As workloads são implementadas com uma estrutura de várias contas e com ambientes separados nessas UOs.

Várias considerações impulsionaram esse design inicial:

- As OUs aninhadas não estavam disponíveis naquele momento AWS Control Tower e exigiam ampla personalização.
- As workloads iniciais designadas para a nuvem se concentraram em aspectos específicos da empresa, como ensaios clínicos ou analytics de equipamentos de manufatura (visualizações funcionais).
- A empresa diferencia entre cinco ambientes de workload (desenvolvimento, validação, integração, treinamento e produção). A empresa precisava de um playground para desenvolver aplicativos sem a governança rígida por meio dos AWS controles exigidos pelas cargas de trabalho de produção. UOs de desenvolvimento, como a Manufacturing-Dev OU, foram designadas para essa finalidade.
- A automação da workload fez parte do ecossistema de cada aplicação e não precisou ser separada.
- Os processos de qualificação de infraestrutura (IQ) e conformidade com GxP não exigiam uma distinção de AWS controles no nível da OU.

Design de UO: fase 2

A empresa farmacêutica, em nosso exemplo, entrou em uma nova fase de maturidade na nuvem ao implantar workloads de produção qualificadas nas UOs existentes. Isso iniciou uma revisão do projeto inicial, e a estrutura da fase 1 foi desafiada à medida que mais cargas de trabalho migraram para a zona AWS de pouso regulamentada.

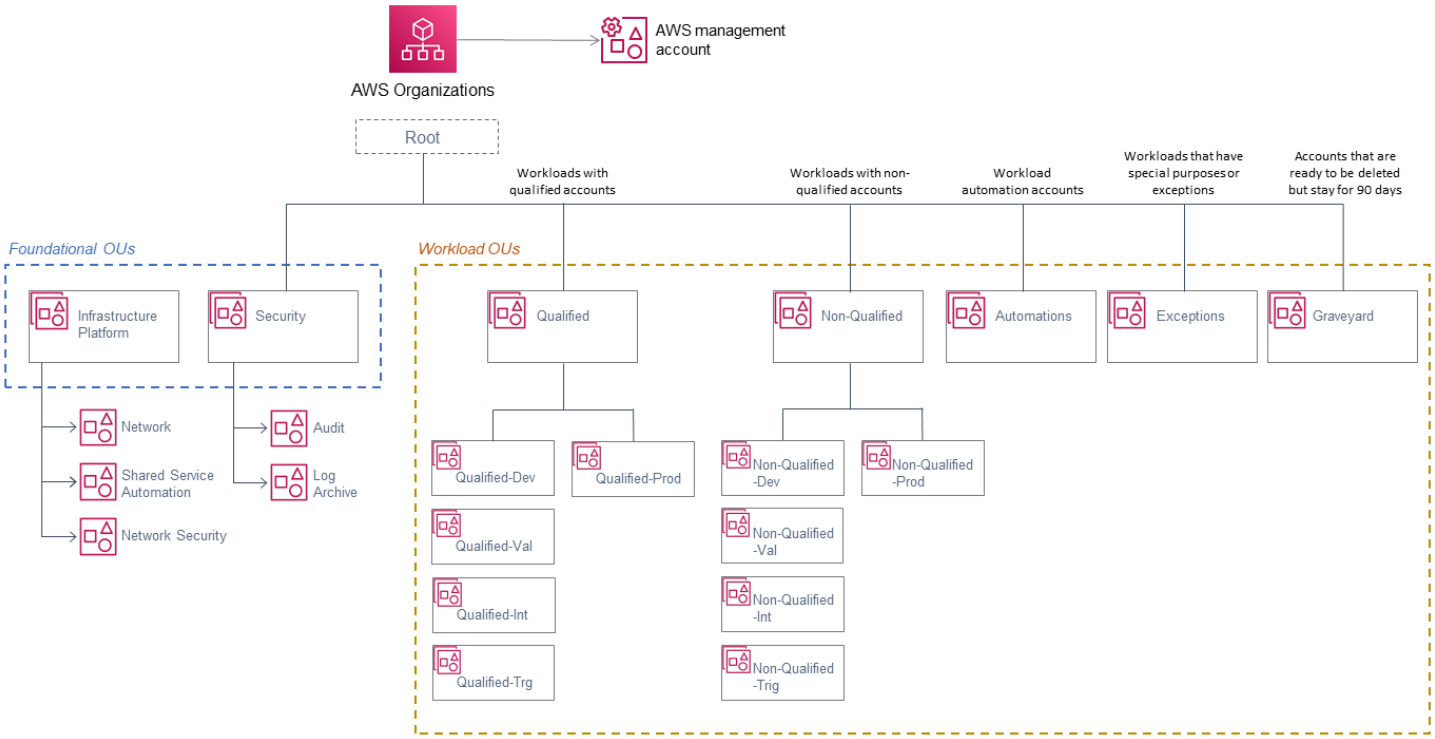
Os seguintes novos requisitos e insights se tornaram importantes:

- A empresa implementou workloads do modelo de compartilhamento de dados, de modo que as aplicações adquiriram uma natureza multifuncional que não podia mais ser atribuída a UOs separadas, como clínicas ou de manufatura.
- A qualificação (em particular, a qualificação contínua) tornou-se um aspecto vital de muitas workloads. Essas workloads precisaram ser integradas aos processos operacionais para que pudessem seguir as práticas recomendadas de segurança com mais facilidade. As cargas de trabalho qualificadas exigiam AWS controles mais rigorosos, que foram definidos no nível da OU na fase 1.
- A funcionalidade de OU aninhada foi disponibilizada em AWS Control Tower.
- A requalificação e a experiência resultaram em uma melhor compreensão de quais políticas específicas eram relevantes para as workloads.
- A empresa definiu e concordou com um modelo operacional baseado no alinhamento de responsabilidades.
- Os esquemas de segmentação e estruturação da workload amadureceram e foram adotados para migrações de workloads.

Como resultado disso, um novo design foi implementado na fase 2 e as Contas da AWS migraram para essa nova estrutura. Essa nova estrutura inclui as UO descritas nas seções a seguir.

Design da arquitetura

O diagrama a seguir mostra a arquitetura da UO da fase 2.



UO de segurança

A OU de segurança contém informações amplamente Contas da AWS relacionadas à funcionalidade de segurança e usa duas contas (auditoria e arquivamento de registros) para armazenar dados operacionais de segurança para acesso central de registros e auditoria ao ambiente. AWS os principais serviços de segurança, como a Amazon GuardDuty , AWS Security Hub CSPM residem na conta de auditoria. Essa UO permanece inalterada em relação ao projeto original.

UO de plataforma de infraestrutura

A Infrastructure Platform OU contém contas de infraestrutura fundamentais, como rede e automação compartilhada em toda a AWS landing zone. Essa UO permanece inalterada em relação ao projeto original.

UO qualificada

A UO qualificada contém workloads que exigem uma infraestrutura qualificada, como gerenciamento rigoroso de alterações, qualificação e validação.

Non-qualified OU

A Non-Qualified OU contém cargas de trabalho que não têm requisitos de GxP ou não são essenciais para os negócios.

UO de automações

O Automations OU contém recursos compartilhados para automação da carga de trabalho, como pipelines de integração contínua e entrega contínua (CI/CD) para gerenciamento de infraestrutura. Dependendo dos requisitos, a automação pode ser dividida entre ambientes ou pode ser hospedada em uma única Conta da AWS.

UO de exceções

A UO de exceções contém workloads que exigem tratamento especial que, de outra forma, seriam evitadas por políticas. Por exemplo, buckets do Amazon Simple Storage Service (Amazon S3), amplamente acessíveis e legíveis, pertencerão à UO de exceções.

UO graveyard

O Graveyard OU contém quatro cargas Contas da AWS de trabalho que serão excluídas. As políticas dessas contas devem ser removidas para um acesso administrativo simples e efetivo até que a conta expire ou seja excluída.

Migração e verificação da UO

Para a empresa farmacêutica multinacional em nosso exemplo, as equipes de engenharia da plataforma de nuvem e gerenciamento de mudanças concordaram com um plano e um cronograma de migração. As Contas da AWS foram analisadas e classificadas de acordo com o impacto e a criticidade nos negócios como parte do planejamento.

A nova estrutura de UO foi implantada lado a lado com a estrutura da UO existente para permitir a preparação de novas políticas e a migração incremental. Criamos novas UOs vazias com UOs secundárias e atribuímos as políticas do AWS Organizations e os controles do AWS Control Tower a essas UOs secundárias.

As políticas do AWS Organizations foram migradas manualmente aplicando-se as políticas desejadas na nova estrutura. Usamos a verificação manual pontual para verificar as políticas do AWS Organizations e mecanismos automatizados para verificar os controles do AWS Control Tower. As Contas da AWS foram migradas para as novas UOs somente depois que essas verificações tiveram êxito.

A migração da conta foi semiautomática e seguiu uma abordagem escalonada ou em lotes. A migração inicial visava as Contas da AWS consideradas menos críticos, usando um lote de cinco Contas da AWS por execução de migração. Os lotes de migração não excederam dez contas. Quando as contas foram migradas, os revisores e testadores usaram o console do AWS Control Tower para verificar se essas contas foram movidas para a UO correta e monitoraram os registros do AWS CloudTrail em busca de erros. Os revisores também verificaram os consoles do AWS Service Catalog e do AWS Control Tower em busca de qualquer desvio ou conta nos estados corrompido ou desconhecido.

As alterações no posicionamento de contas na UO não afetaram a conectividade ou a acessibilidade dos recursos. Nenhuma interrupção em uma aplicação de produção foi relatada.

Lições aprendidas e práticas recomendadas

- O design da estrutura da UO não é um esforço único. À medida que uma empresa aumenta a adoção da nuvem e migra workloads adicionais para a zona de pouso da AWS, seu design de UO (e implicitamente seu conceito de políticas) também evoluirá naturalmente.
- Não confunda UOs com pastas; considere-asum alvo para políticas. As UOs e sua hierarquia fornecem o elemento estruturante das Contas da AWS e devem sempre ser tratadas como contêineres para políticas. Recomendamos que você coloque tudas as Contas da AWS que exigem o mesmo conjunto de políticas na mesma UO. Essa diretriz também se estende às UOs aninhadas (UOs dentro de UOs).

  Os ambientes da AWS que exigem funcionalidade compartilhada de forma centralizada e recursos de compartilhamento de dados entre workloads (que são frequentemente vistos em plataformas de dados corporativos) são mais fáceis de acomodar em uma estrutura de UO que não se baseia na classificação de funções de linhas de negócios (LOB). Por exemplo, um ambiente de produção para uma aplicação de manufatura não é diferente de um ambiente de produção para uma aplicação de analytics de ensaios clínicos em termos de políticas no AWS Organizations.
- Respeite e use a herança. Quando você anexa uma política a uma UO específica, as Contas da AWS que estão diretamente sob essa UO ou qualquer UO secundária herdam a política. Quando você anexa uma política a uma Conta da AWS específica, ela afeta apenas essa Conta da AWS.

  O esforço de migração de uma estrutura de UO para outra depende de quão extensivamente as políticas existentes foram configuradas na UO ou no nível da Conta da AWS. Outro fator crucial é o grau de herança de políticas na hierarquia atual de UOs existentes, ou se a herança foi interrompida. A complexidade da migração aumenta com a implementação de caminhos de herança irregulares ou divergentes. Por exemplo, se você aplicar políticas no nível individual de Conta da AWS ou fizer exceções de políticas frequentes (que quebram a herança), migrar essas políticas para uma nova estrutura exigirá muito mais esforço. Nesses casos de alta complexidade, recomendamos que você invista tempo para revisar e redesenhar a herança de políticas durante o planejamento da migração.
- Cuide das políticas do AWS Organizations e dos controles do AWS Control Tower. A estrutura da UO é compartilhada entre o AWS Control Tower e o AWS Organizations. O AWS Control Tower fornece seu próprio conjunto de controles preventivos e de detecção. Esses controles são aplicados no nível da Conta da AWS ou da UO. O AWS Organizations orquestra políticas no nível da UO. Em uma migração de UO, recomendamos que você migre as políticas do AWS

Organizations primeiro, porque elas têm mais peso para a conformidade. Recomendamos que você aplique os controles do AWS Control Tower à nova estrutura de UO na segunda etapa de migração.

- Leva algum tempo para a atualização das Contas da AWS. Você deve inscrever novamente as Contas da AWS existentes individualmente na nova estrutura da UO usando o AWS Control Tower. Isso leva algum tempo. Se você tiver um grande número de contas, recomendamos otimizar esse trabalho por meio de automação para controlar e automatizar o posicionamento das UO das Contas da AWS. Confira dois exemplos de cenários:
  - Alteração manual para uma pequena migração: o líder da migração reatribui cada Conta da AWS de sua antiga UO para sua nova UO no Console de gerenciamento da AWS. Quando essa reatribuição é concluída para todas as Contas da AWS, o líder de migração abre o AWS Control Tower para cada Conta da AWS separadamente ou para todas as UOs. A nova inscrição das Contas da AWS no AWS Control Tower requer de 10 a 15 minutos para cada Conta da AWS, dependendo do número de Regiões da AWS usadas na conta. O AWS Control Tower permite que até cinco operações simultâneas desse tipo sejam executadas em paralelo.
  - Automação personalizada de alterações: a automação simplifica e economiza esforços. Por exemplo, você pode automatizar o gerenciamento de um ciclo de vida da Conta da AWS desde sua criação até a migração e o encerramento. Você pode usar o AWS Control Tower Account Factory para alterar a atribuição da UO para uma Conta da AWS e executar o processo de nova inscrição. Essa automação é compatível com a migração em grande escala de centenas de Contas da AWS.

Recursos

- Guia do usuário do AWS Organizations (documentação da AWS)
- Terminologia e conceitos do AWS Organizations (documentação da AWS)
- Service control policies (SCPs) (documentação da AWS)
- AWS Organizations API reference (documentação da AWS)
- Guia do usuário do AWS Control Tower (documentação da AWS)
- Introducing Landing Zone Accelerator for Healthcare (publicação do Blog da AWS)
- Managing the multi-account environment using AWS Organizations and AWS Control Tower (publicação do Blog da AWS)
- Best Practices for Organizational Units with AWS Organizations (publicação do Blog da AWS)
- AWS Security Reference Architecture (AWS SRA) (Recomendações da AWS)
- Establishing Your Cloud Foundation on AWS (whitepaper da AWS)
- Organizing Your AWS Environment Using Multiple Accounts (whitepaper da AWS)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	28 de março de 2023

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.