Struktur OU di zona AWS pendaratan yang diatur: contoh dari industri farmasi

AWS Panduan Preskriptif

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Panduan Preskriptif: Struktur OU di zona AWS pendaratan yang diatur: contoh dari industri farmasi

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Pengantar 1
Gambaran umum 2
  Jenis kebijakan 2
Desain OU: fase 1 4
  Desain arsitektur 4
  Keamanan OU 4
  Platform Infrastruktur OU 5
  OU tambahan 5
Desain OU: fase 2 6
  Desain arsitektur 6
  Keamanan OU 7
  Platform Infrastruktur OU 7
  OU yang memenuhi syarat 7
  Non-qualified OU 8
  Otomatisasi OU 8
  Pengecualian OU 8
  Makam OU 8
Migrasi dan verifikasi OU 9
Pelajaran yang dipetik dan praktik terbaik 10
Sumber daya 12
Riwayat dokumen 13
 xiv

Struktur OU di zona AWS pendaratan yang diatur: contoh dari industri farmasi

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

Maret 2023 (sejarah dokumen)

AWS menyediakan beberapa konfigurasi Akselerator Zona Pendaratan yang mendukung industri tertentu, termasuk perawatan kesehatan. Akselerator Zona Pendaratan untuk Perawatan Kesehatan digunakan bersama AWS Control Tower untuk memudahkan pengelolaan dan tata kelola lingkungan multi-akun yang selaras dengan praktik AWS terbaik dan beberapa kerangka kerja kepatuhan global. Salah satu aspek penting dari mengatur tata kelola adalah mengelompokkan Akun AWS bersama dengan menggunakan unit organisasi (OUs), sehingga Anda dapat mengelolanya sebagai satu kesatuan.

Panduan ini membahas praktik dan pertimbangan terbaik untuk mendesain ulang struktur OU yang ada saat kematangan cloud perusahaan Anda tumbuh. Ini memperkenalkan contoh praktis berdasarkan AWS Control Tower implementasi untuk perusahaan farmasi besar, dan membahas pelajaran yang didapat dari implementasi itu. AWS desain landing zone bukanlah upaya satu kali. Itu bisa dan harus dibiarkan berkembang. Evolusi ini dapat berhasil dan efisien dicapai dengan menerapkan praktik dan tip AWS terbaik yang disorot dalam panduan ini.

Gambaran umum

Kami bekerja dengan perusahaan farmasi multinasional untuk menjalankan kegiatan proof-of-concept (PoC) AWS untuk mengeksplorasi bagaimana mereka dapat memigrasikan aplikasi mereka dari tempat ke tempat. AWS Cloud Ketika mereka mulai menskalakan dan mempercepat alur kerja migrasi mereka untuk memasukkan beban kerja produksi, menjadi jelas bahwa mereka membutuhkan landing AWS zone yang diatur dan sesuai untuk mendukung tujuan mereka. Kami dulu AWS Control Towermerancang dan mengimplementasikan AWS landing zone baru.

Aspek penting dari AWS landing zone baru dan organisasinya adalah struktur unit organisasinya (OUs). OU adalah pengelompokan logis yang Akun AWS dibuat dengan menggunakan AWS Organizations. Anda dapat menggunakannya OUs untuk mengatur Akun AWS ke dalam hierarki dan menerapkan kontrol manajemen dan tata kelola secara konsisten dan lebih mudah.

Anda dapat melampirkan kontrol berbasis kebijakan ke OU dan ke. Akun AWS Anak OUs dalam OU secara otomatis mewarisi kontrol tersebut. Oleh karena itu, OUs memainkan peran penting dalam mengelola keamanan dan tata kelola di AWS Organizations.

Kebijakan adalah dokumen JSON yang menyertakan satu atau beberapa pernyataan yang menentukan kontrol yang ingin Anda terapkan ke grup. Akun AWS AWS Organizations Saat ini mendukung empat jenis kebijakan, juga dikenal sebagai kebijakan kontrol layanan (SCPs). SCP mendefinisikan Layanan AWS dan tindakan yang tersedia untuk digunakan secara berbeda. Akun AWS Misalnya, Anda dapat menggunakan SCP untuk meminta peluncuran instans Amazon Elastic Compute Cloud EC2 (Amazon) agar menggunakan jenis instans tertentu.

Jenis kebijakan

Jenis kebijakan SCP meliputi:

- Izinkan daftar dan tolak daftar adalah strategi pelengkap yang dapat Anda gunakan SCPs untuk diterapkan untuk memfilter izin yang tersedia untuk akun.
- Kebijakan tag membantu Anda mempertahankan tag yang konsisten, termasuk perlakuan kasus yang disukai dari kunci tag dan nilai tag di seluruh akun.
- Kebijakan cadangan mengonfigurasi pencadangan untuk jenis sumber daya yang didukung, seperti jendela waktu cadangan dan brankas tujuan untuk pencadangan. Wilayah AWS
- Kebijakan opt-out layanan AI memungkinkan atau menonaktifkan peningkatan berkelanjutan layanan kecerdasan AWS buatan (AI) secara global.

Perilaku pewarisan kebijakan: Saat Anda melampirkan kebijakan ke OU tertentu, akun yang secara langsung berada di bawah OU tersebut atau OU anak mana pun mewarisi kebijakan tersebut. Saat Anda melampirkan kebijakan ke akun tertentu, kebijakan tersebut hanya memengaruhi akun tersebut. Anda dapat menimpa kebijakan yang diwariskan dengan memperkenalkan kebijakan pengecualian. Warisan secara eksplisit memungkinkan semua izin mengalir dari root (OU) ke setiap Akun AWS OU dan OU anak itu, kecuali jika Anda secara eksplisit menolak izin. Untuk menolak izin, Anda membuat kebijakan tambahan dan melampirkannya ke OU yang sesuai atau Akun AWS. Untuk informasi selengkapnya tentang pewarisan kebijakan dan pengecualian, lihat dokumentasi.AWS Organizations

AWS Control Tower juga menyediakan set kontrol detektif dan preventif sendiri (juga disebut pagar pembatas) dengan menggunakan struktur OU. AWS Control Tower kontrol preventif mencegah tindakan dengan menggunakan SCPs in AWS Organizations. Detective control melaporkan penyimpangan konfigurasi terhadap kontrol dengan menggunakan. AWS Config Untuk informasi selengkapnya tentang kontrol ini, lihat AWS Control Tower dokumentasi.

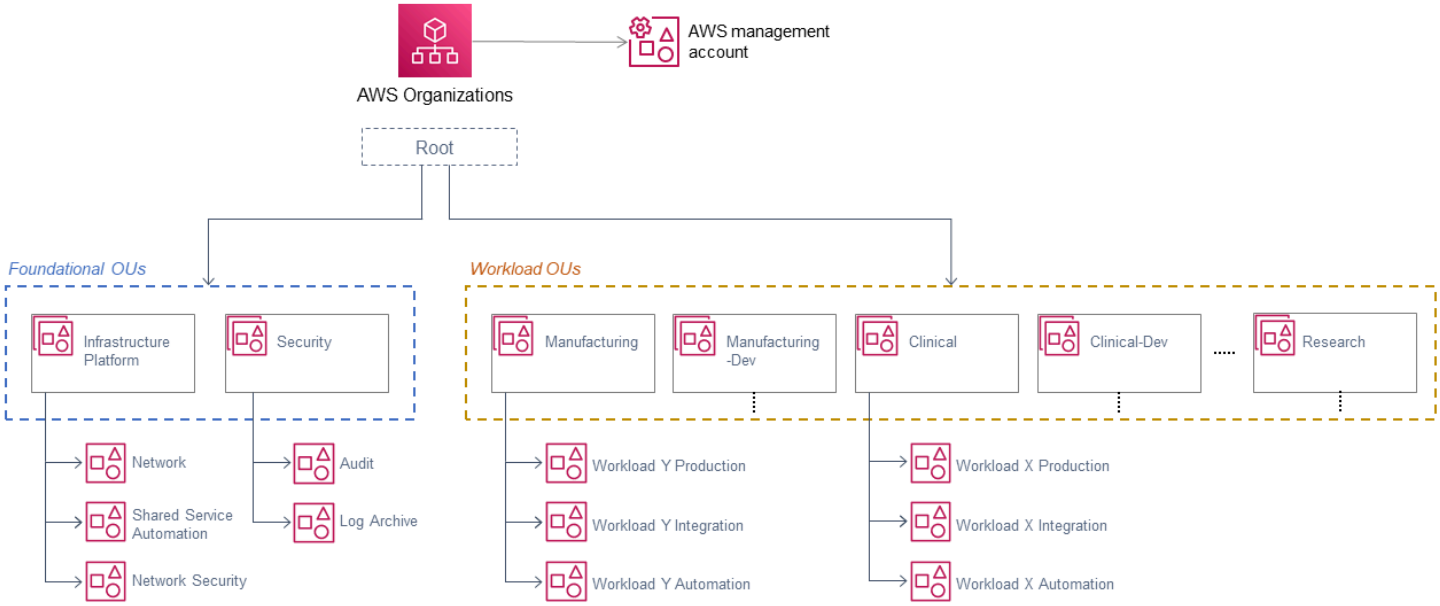
Anda juga dapat mengaktifkan AWS Security Hub CSPMuntuk mengotomatiskan pemeriksaan praktik terbaik keamanan, menggabungkan peringatan keamanan ke dalam satu tempat dan format, dan memahami postur keamanan secara keseluruhan di semua tempat Anda. Akun AWS

Desain OU: fase 1

Untuk perusahaan farmasi multinasional dalam contoh kami, desain awal organisasi dan OU dalam AWS rekomendasi yang diikuti AWS Organizations dengan cermat untuk pengaturan. AWS Control Tower Sebagai contoh, lihat Akselerator Zona Pendaratan AWS untuk Perawatan Kesehatan. AWS Control Tower awalnya menyediakan struktur OU sederhana dengan OU dasar umum, seperti yang dijelaskan dalam posting blog Praktik Terbaik untuk Unit Organisasi dengan AWS Organizations, termasuk OU Keamanan, OU Infrastruktur Platform, dan OU khusus perusahaan.

Desain arsitektur

Diagram berikut menunjukkan arsitektur OU awal.



Keamanan OU

Security OU mengelompokkan secara luas Akun AWS terkait dengan fungsi keamanan bersama-sama dan menggunakan dua akun (Audit dan Log Archive) untuk menyimpan data operasional keamanan untuk pencatatan pusat dan akses audit ke lingkungan. AWS layanan keamanan inti seperti Amazon GuardDuty dan AWS Security Hub CSPM berada di akun Audit.

Platform Infrastruktur OU

Platform Infrastruktur OU mengelompokkan bersama Akun AWS yang menyediakan fondasi infrastruktur. Awalnya digunakan dalam OU ini adalah Akun AWS untuk komponen jaringan pusat (gateway, firewall, hub jaringan pusat, dan layanan serupa).

OU tambahan

OU khusus perusahaan lainnya (seperti OU Klinis) menambah OU dasar dalam hierarki tingkat rendah. Beban kerja diimplementasikan dengan struktur multi-akun dan dengan lingkungan terpisah di dalam OU tersebut.

Beberapa pertimbangan mendorong desain awal ini:

- OU bersarang tidak tersedia pada saat itu AWS Control Tower dan membutuhkan penyesuaian ekstensif.
- Beban kerja awal yang ditujukan untuk cloud berfokus pada aspek-aspek tertentu dari perusahaan seperti uji klinis atau analitik peralatan manufaktur (tampilan fungsional).
- Perusahaan membedakan antara lima lingkungan beban kerja (pengembangan, validasi, integrasi, pelatihan, dan produksi). Perusahaan membutuhkan taman bermain untuk mengembangkan aplikasi tanpa tata kelola yang ketat dengan AWS mengontrol beban kerja produksi yang diperlukan. Pengembangan OU seperti Manufacturing-Dev OU ditugaskan untuk tujuan ini.
- Otomatisasi beban kerja adalah bagian dari ekosistem masing-masing aplikasi dan tidak perlu dipisahkan.
- Kualifikasi infrastruktur (IQ) dan proses kepatuhan GxP tidak memerlukan perbedaan AWS kontrol di tingkat OU.

Desain OU: fase 2

Perusahaan farmasi dalam contoh kami berakselerasi ke fase baru kematangan cloud dengan menerapkan beban kerja produksi yang memenuhi syarat ke dalam OU yang ada. Ini memulai tinjauan desain awal, dan struktur fase 1 ditantang karena lebih banyak beban kerja bermigrasi ke landing zone yang diatur. AWS

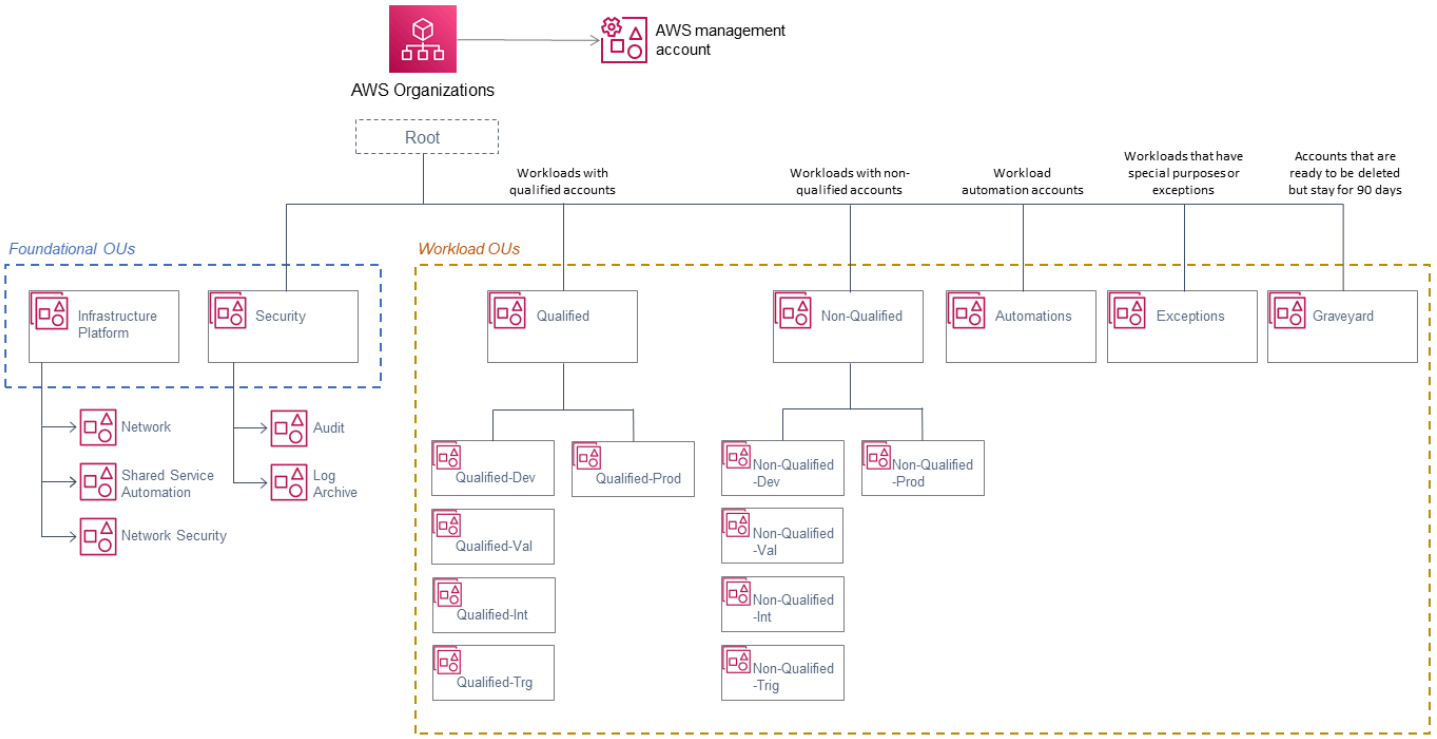
Persyaratan dan wawasan baru berikut menjadi penting:

- Perusahaan menerapkan beban kerja model berbagi data, sehingga aplikasi memperoleh sifat multi-tujuan yang tidak dapat lagi ditugaskan untuk memisahkan OU seperti Klinis atau Manufaktur.
- Kualifikasi (khususnya, kualifikasi berkelanjutan) menjadi aspek vital dari banyak beban kerja. Beban kerja ini harus diintegrasikan ke dalam proses operasional sehingga mereka dapat mengikuti praktik terbaik keamanan dengan lebih mudah. Beban kerja yang memenuhi syarat membutuhkan AWS kontrol yang lebih ketat, yang ditetapkan pada tingkat OU di fase 1.
- Fungsionalitas OU bersarang menjadi tersedia di AWS Control Tower.
- Peningkatan keterampilan dan pengalaman menghasilkan pemahaman yang lebih baik tentang kebijakan spesifik mana yang relevan untuk beban kerja.
- Perusahaan mendefinisikan dan menyetujui model operasional yang didasarkan pada penyelarasan tanggung jawab.
- Segmentasi beban kerja dan cetak biru penataan matang dan diadopsi untuk migrasi beban kerja.

Sebagai hasilnya, desain baru diimplementasikan pada fase 2 dan Akun AWS bermigrasi ke struktur baru itu. Struktur baru ini mencakup OU yang dijelaskan di bagian berikut.

Desain arsitektur

Diagram berikut menunjukkan arsitektur OU untuk fase 2.



Keamanan OU

OU Keamanan berisi secara luas Akun AWS terkait dengan fungsionalitas keamanan dan menggunakan dua akun (Audit dan Arsip Log) untuk menyimpan data operasional keamanan untuk pencatatan pusat dan akses audit ke lingkungan. AWS layanan keamanan inti seperti Amazon GuardDuty dan AWS Security Hub CSPM berada di akun audit. OU ini tetap tidak berubah dari desain aslinya.

Platform Infrastruktur OU

Platform Infrastructure OU berisi akun infrastruktur dasar seperti jaringan dan otomatisasi bersama di seluruh AWS landing zone. OU ini tetap tidak berubah dari desain aslinya.

OU yang memenuhi syarat

The Qualified OU berisi beban kerja yang membutuhkan infrastruktur yang berkualitas seperti manajemen perubahan yang ketat, kualifikasi, dan validasi.

Non-qualified OU

Non-Qualified OU berisi beban kerja yang tidak memiliki persyaratan GxP atau tidak penting bagi bisnis.

Otomatisasi OU

Automations OU berisi sumber daya bersama untuk otomatisasi beban kerja, seperti integrasi berkelanjutan dan jalur pipa pengiriman berkelanjutan (CI/CD) untuk manajemen infrastruktur. Bergantung pada persyaratan, otomatisasi dapat dibagi di seluruh lingkungan atau dihosting dalam satu Akun AWS.

Pengecualian OU

Pengecualian OU berisi beban kerja yang memerlukan perlakuan khusus yang seharusnya dicegah oleh kebijakan. Misalnya, bucket Amazon Simple Storage Service (Amazon S3) yang dapat diakses secara luas dan dapat dibaca akan termasuk dalam Exceptions OU.

Makam OU

Graveyard OU berisi Akun AWS beban kerja yang akan dihapus. Kebijakan dalam akun ini harus dihapus untuk akses administratif yang efektif dan sederhana sampai akun kedaluwarsa atau dihapus.

Migrasi dan verifikasi OU

Untuk perusahaan farmasi multinasional dalam contoh kami, tim rekayasa platform cloud dan manajemen perubahan menyetujui rencana dan jadwal migrasi. Akun AWS ditinjau dan diberi peringkat berdasarkan dampak bisnis dan kekritisan sebagai bagian dari perencanaan.

Struktur OU baru dikerahkan berdampingan dengan struktur OU yang ada untuk memungkinkan pementasan kebijakan baru dan migrasi bertahap. Kami membuat kosong baru OUs dengan anak OUs dan menetapkan AWS Organizations kebijakan serta AWS Control Tower kontrol untuk anak tersebut OUs.

AWS Organizations Kebijakan dimigrasikan secara manual dengan menerapkan kebijakan yang diinginkan pada struktur baru. Kami menggunakan pemeriksaan spot manual untuk memverifikasi AWS Organizations kebijakan dan mekanisme otomatis untuk memverifikasi AWS Control Tower kontrol. Akun AWS dipindahkan ke yang baru OUs hanya setelah pemeriksaan ini berhasil.

Migrasi akun semi-otomatis dan mengikuti pendekatan terhuyung-huyung atau batch. Migrasi awal ditargetkan Akun AWS yang dianggap kurang kritis, menggunakan batch lima Akun AWS per migrasi yang dijalankan. Batch migrasi tidak melebihi 10 akun. Ketika akun dimigrasikan, pengulas dan penguji menggunakan AWS Control Tower konsol untuk memverifikasi bahwa akun ini dipindahkan ke OU yang benar dan log yang dipantau AWS CloudTrail untuk kesalahan. Peninjau juga memeriksa AWS Service Catalog dan AWS Control Tower konsol untuk setiap penyimpangan atau akun di negara bagian yang tercemar atau tidak dikenal.

Perubahan penempatan akun OU tidak memengaruhi konektivitas atau aksesibilitas sumber daya. Tidak ada pemadaman dalam aplikasi produksi yang dilaporkan.

Pelajaran yang dipetik dan praktik terbaik

- Desain struktur OU bukanlah upaya satu kali. Ketika perusahaan meningkatkan adopsi cloud dan memigrasikan beban kerja tambahan ke AWS landing zone, desain OU (dan secara implisit konsep kebijakannya) juga akan berkembang secara alami.
- Jangan salah OUs untuk folder; anggap mereka target untuk kebijakan. Hirarki OUs dan mereka menyediakan elemen penataan untuk Akun AWS dan harus selalu diperlakukan sebagai wadah untuk kebijakan. Kami menyarankan Anda menempatkan semua Akun AWS yang memerlukan serangkaian kebijakan yang sama ke dalam OU yang sama. Pedoman ini juga meluas ke nested OUs (OUs dalam). OUs

  AWS lingkungan yang membutuhkan fungsionalitas bersama terpusat dan kemampuan berbagi data lintas beban kerja (yang sering terlihat di platform data perusahaan) lebih mudah diakomodasi dalam struktur OU yang tidak didasarkan pada klasifikasi fungsi lini bisnis (LOB). Misalnya, lingkungan produksi untuk aplikasi manufaktur tidak berbeda dengan lingkungan produksi untuk aplikasi analisis uji klinis dalam hal kebijakan di AWS Organizations.
- Hormati dan gunakan warisan. Ketika Anda melampirkan kebijakan ke OU tertentu, Akun AWS yang secara langsung berada di bawah OU tersebut atau di bawah anak mana pun, OU mewarisi kebijakan tersebut. Saat Anda melampirkan kebijakan ke kebijakan tertentu Akun AWS, kebijakan hanya memengaruhi itu Akun AWS.

  Upaya migrasi dari satu struktur OU ke struktur lain tergantung pada seberapa luas kebijakan yang ada dikonfigurasi di OU atau Akun AWS tingkat. Faktor penting lainnya adalah berapa banyak pewarisan kebijakan yang digunakan dalam hierarki OU yang ada, atau jika pewarisan rusak. Kompleksitas migrasi meningkat dengan penerapan jalur pewarisan yang tidak teratur atau menyimpang. Misalnya, jika Anda menerapkan kebijakan di Akun AWS tingkat individu atau sering membuat pengecualian kebijakan (yang melanggar warisan), memigrasikan kebijakan tersebut ke dalam struktur baru akan membutuhkan upaya yang jauh lebih besar. Dalam kasus kompleksitas tinggi seperti itu, kami menyarankan Anda menginvestasikan waktu untuk meninjau dan mendesain ulang warisan kebijakan selama perencanaan migrasi.
- Jaga AWS Organizations kebijakan dan AWS Control Tower kontrol. Struktur OU dibagi antara AWS Control Tower dan AWS Organizations. AWS Control Tower menyediakan set kontrol detektif dan preventif sendiri. Kontrol ini berlaku di tingkat Akun AWS atau OU. AWS Organizations mengatur kebijakan di tingkat OU. Dalam migrasi OU, kami menyarankan Anda untuk memigrasikan AWS Organizations kebijakan terlebih dahulu, karena kebijakan ini lebih

membebani kepatuhan. Kami menyarankan Anda menerapkan AWS Control Tower kontrol ke struktur OU baru di langkah migrasi kedua.

- Butuh waktu untuk memperbarui Akun AWS. Anda harus mendaftarkan ulang yang ada Akun AWS secara individual ke dalam struktur OU baru dengan menggunakan. AWS Control Tower Ini membutuhkan waktu. Jika Anda memiliki banyak akun, kami sarankan Anda merampingkan pekerjaan ini melalui otomatisasi untuk mengontrol dan mengotomatiskan penempatan OU. Akun AWS Berikut adalah dua contoh skenario:
  - Perubahan manual untuk migrasi kecil: Pimpinan migrasi menetapkan kembali masing-masing Akun AWS dari OU lamanya ke OU barunya di Konsol Manajemen AWS. Ketika penugasan kembali itu selesai untuk semua Akun AWS, petunjuk migrasi terbuka AWS Control Tower baik untuk masing-masing Akun AWS secara terpisah atau untuk semua. OUs Mendaftar ulang Akun AWS AWS Control Tower membutuhkan 10-15 menit untuk masing-masing Akun AWS tergantung pada jumlah yang Wilayah AWS digunakan dalam akun. AWS Control Tower memungkinkan hingga lima operasi bersamaan semacam ini berjalan secara paralel.
  - Otomatisasi perubahan kustom: Otomasi menyederhanakan dan menghemat usaha. Misalnya, Anda dapat mengotomatiskan pengelolaan Akun AWS siklus hidup dari pembuatannya hingga migrasi dan penghentian. Anda dapat menggunakan AWS Control Tower Account Factory untuk mengubah penetapan OU untuk Akun AWS dan menjalankan proses pendaftaran ulang. Otomatisasi ini mendukung migrasi skala besar ratusan Akun AWS.

Sumber daya

- AWS Organizations Panduan Pengguna (AWS dokumentasi)
- AWS Organizations terminologi dan konsep (AWS dokumentasi)
- Kebijakan kontrol layanan (SCPs) (AWS dokumentasi)
- AWS Organizations Referensi API (AWS dokumentasi)
- AWS Control Tower Panduan Pengguna (AWS dokumentasi)
- Memperkenalkan Akselerator Zona Pendaratan untuk Perawatan Kesehatan (posting AWS blog)
- Mengelola lingkungan multi-akun menggunakan AWS Organizations dan AWS Control Tower (posting AWS blog)
- Praktik Terbaik untuk Unit Organisasi dengan AWS Organizations (posting AWS blog)
- AWS Arsitektur Referensi Keamanan (AWS SRA) (PanduanAWS Preskriptif)
- Membangun Cloud Foundation Anda di AWS (AWS whitepaper)
- Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun (AWS whitepaper)

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Maret 28, 2023

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.