aws

Panduan Pengguna

Rekomendasi Strategi Migrasi Hub

Rekomendasi Strategi Migrasi Hub: Panduan Pengguna

Table of Contents

Apa itu Rekomendasi Strategi Migrasi Hub?

Rekomendasi Strategi Hub Migrasi membantu Anda merencanakan inisiatif migrasi dan modernisasi dengan menawarkan rekomendasi strategi migrasi dan modernisasi untuk jalur transformasi yang layak untuk aplikasi Anda.

Rekomendasi Strategi dapat menganalisis inventaris server Anda, lingkungan runtime, dan binari aplikasi untuk aplikasi Microsoft IIS dan Java Tomcat dan Jboss untuk menghasilkan laporan anti-pola. Selain itu, Anda dapat mengonfigurasi kode sumber Anda untuk memungkinkan Rekomendasi Strategi melakukan kode sumber dan analisis basis data semua aplikasi Anda. Rekomendasi Strategi membandingkan analisis ini dengan tujuan bisnis Anda, dan preferensi transformasi aplikasi dan database yang Anda berikan untuk direkomendasikan:

- Strategi migrasi paling efektif untuk setiap aplikasi Anda.
- Alat atau layanan migrasi dan modernisasi yang dapat Anda gunakan.
- Ketidakcocokan aplikasi dan anti-pola untuk menyelesaikan opsi tertentu.

Rekomendasi Strategi Migration Hub merekomendasikan strategi migrasi dan modernisasi untuk rehosting, replatforming, dan refactoring dengan tujuan, alat, dan program penyebaran terkait. Untuk informasi tentang rehosting, replatforming, dan refactoring, lihat Istilah migrasi - 7 Rs di glosarium Panduan Preskriptif. AWS

Rekomendasi Strategi mungkin merekomendasikan opsi langsung, seperti rehosting di Amazon Elastic Compute Cloud (Amazon EC2AWS) menggunakan Application Migration Service (MGN). AWS Rekomendasi yang lebih dioptimalkan mungkin termasuk replatforming ke container menggunakan AWS App2Container, atau refactoring ke teknologi open source seperti .NET Core dan PostgreSQL.

Apakah Anda pelanggan Rekomendasi Strategi pertama kali?

Jika ini adalah pertama kalinya Anda menggunakan Rekomendasi Strategi, kami sarankan Anda mulai dengan membaca bagian berikut:

- Ikhtisar Rekomendasi Strategi
- Menyiapkan Rekomendasi Strategi
- Memulai dengan Rekomendasi Strategi

Ikhtisar Rekomendasi Strategi

Anda dapat memulai penilaian untuk portofolio server dan aplikasi Anda dengan menggunakan Rekomendasi Strategi Hub Migrasi dari AWS Migration Hub konsol. Anda menggunakan konsol untuk mengatur dan melakukan penilaian. Setelah penilaian, Anda dapat menggunakan konsol untuk melihat data penilaian untuk setiap server dan aplikasi, bersama dengan alat transformasi yang direkomendasikan.

Untuk menerima rekomendasi refactoring dan daftar ketidakcocokan, Anda dapat menggunakan Rekomendasi Strategi untuk menilai kode sumber dan database aplikasi Anda.

Anda juga dapat mengunduh data rekomendasi dalam file Microsoft Excel.

Layanan terkait

- AWS Migration Hub— Anda menggunakan AWS Migration Hub konsol untuk mengakses konsol Rekomendasi Strategi Migration Hub. Ini juga menampilkan informasi tentang server tempat Anda mengumpulkan data.
- AWS Application Discovery ServiceAnda menggunakan Application Discovery Service untuk mengumpulkan data tentang server dan aplikasi Anda di AWS Migration Hub konsol sebelum menggunakan Rekomendasi Strategi.
- AWSLayanan Migrasi AWS Aplikasi — Layanan Migrasi Aplikasi adalah layanan migrasi utama yang direkomendasikan untuk lift-and-shift AWS migrasi.
- AWS Database Migration Service— AWS Database Migration Service adalah layanan web yang dapat Anda gunakan untuk memigrasikan data dari database lokal, pada instans DB Amazon Relational Database Service (Amazon RDS), atau dalam database di instans Amazon Elastic Compute Cloud (Amazon EC2) ke database pada layanan. AWS
- AWSApp2Container — AWS App2Container (A2C) adalah alat baris perintah untuk memodernisasi aplikasi.NET dan Java ke dalam aplikasi container.
- Porting Assistant untuk.NET — Gunakan untuk analisis kode sumber.NET. Porting Assistant untuk.NET adalah pemindai kompatibilitas yang mengurangi upaya manual yang diperlukan untuk mem-port aplikasi Microsoft .NET Framework ke .NET Core. Porting Assistant untuk.NET menilai kode sumber aplikasi.NET dan mengidentifikasi API yang tidak kompatibel dan paket pihak ketiga.
- Program Migrasi Akhir Dukungan untuk Windows Server - Program Migrasi Akhir Dukungan (EMP) untuk Windows Server mencakup perkakas untuk memigrasi aplikasi lama Anda dari Windows

Server 2003, 2008, dan 2008 R2 ke versi yang lebih baru dan didukung, tanpa refactoring apa pun. AWS

- AWSSchema Conversion Tool — Anda dapat menggunakan AWS Schema Conversion Tool AWS SCT () untuk mengonversi skema database yang ada dari satu mesin database ke mesin database lainnya.
- Asisten Migrasi Aplikasi Web Windows - Asisten Migrasi Aplikasi Web Windows untuk AWS Elastic Beanstalk adalah PowerShell utilitas interaktif yang memigrasikan aplikasi ASP.NET dan ASP.NET Core dari server Windows IIS lokal ke Elastic Beanstalk.
- Babelfish untuk Aurora PostgreSQL — Babelfish for Aurora PostgreSQL adalah kemampuan baru untuk Amazon Aurora PostgreSQL Edisi yang kompatibel dengan Amazon Aurora yang memungkinkan Aurora memahami perintah dari aplikasi yang ditulis untuk server Microsoft SQL.

Menyiapkan Rekomendasi Strategi

Sebelum Anda menggunakan Rekomendasi Strategi Hub Migrasi untuk pertama kalinya, selesaikan tugas berikut:

Topik

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua AWS services dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Rekomendasi Strategi pengguna dan peran

Kami menyarankan Anda membuat dua peran untuk Rekomendasi Strategi:

- Untuk mengakses konsol, buat peran dengan kebijakan `AWSMigrationHubFullAccess` dan kebijakan `AWSMigrationHubStrategyConsoleFullAccess` terkelola yang dilampirkan.
- Untuk mengakses pengumpul data aplikasi Rekomendasi Strategi, buat peran dengan kebijakan `AWSMigrationHubStrategyCollector` terkelola terlampir.

Kebijakan terkelola IAM menentukan tingkat akses ke layanan oleh pengguna. Kebijakan AWS Migration Hub `AWSMigrationHubFullAccess` terkelola memberikan akses ke konsol Migration Hub. Untuk informasi selengkapnya, lihat Peran dan Kebijakan Hub Migrasi. Untuk informasi tentang `AWSMigrationHubStrategyConsoleFullAccess` dan kebijakan yang `AWSMigrationHubStrategyCollector` dikelola, lihatAWS kebijakan terkelola untuk Rekomendasi Strategi Hub Migrasi.

Untuk memberikan akses, menambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin di Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Membuat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Memulai dengan Rekomendasi Strategi

Bagian ini menjelaskan cara memulai Rekomendasi Strategi Migration Hub.

Topik

Prasyarat untuk Rekomendasi Strategi

Berikut ini adalah prasyarat untuk menggunakan Rekomendasi Strategi Migration Hub.

- Anda harus memiliki satu atau beberapa AWS akun, dan pengguna mengatur akun ini. Untuk informasi selengkapnya, lihat Menyiapkan Rekomendasi Strategi.
- Klien pengumpul data aplikasi Rekomendasi Strategi harus dapat mengumpulkan data dari jarak jauh dari server. Ini mengharuskan Anda menggunakan satu set kredensil yang berfungsi untuk semua server Windows Anda dan satu set kredensil yang berfungsi untuk semua server Linux Anda. Kredensi harus memiliki izin untuk membuat dan menghapus direktori di server Anda.
- Versi kolektor yang digunakan di vCenter mendukung VMware vCenter Server V6.0, V6.5, 6.7 atau 7.0.

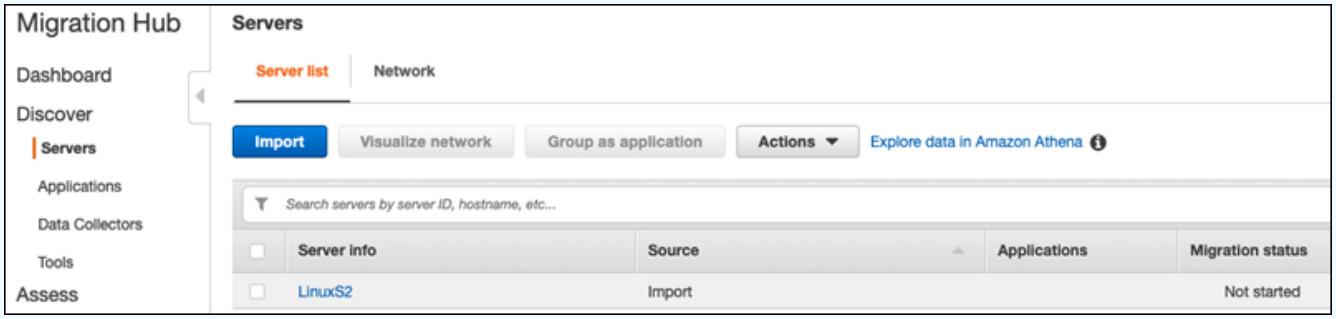
  Anda juga dapat menyebarkan kolektor di instans Amazon EC2 menggunakan AMI kolektor.
- Verifikasi bahwa lingkungan sistem operasi (OS) Anda didukung:
  - Linux
    - Amazon Linux 2012.03, 2015.03
    - Amazon Linux 2 (pembaruan 9/25/2018 dan yang lebih baru)
    - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04
    - Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1

    - CentOS 5.11, 6.9, 7.3
    - SUSE 11 SP4, 12 SP5
  - Windows
    - Windows Server 2008 R1 SP2, 2008 R2 SP1
    - Windows Server 2012 R1, 2012 R2
    - Windows Server 2016
    - Windows Server 2019
- Untuk analisis kode sumber, repositori Anda GitHub dan GitHub Enterprise harus memiliki token akses pribadi dengan lingkup repo yang dapat dibagikan dengan klien kolektor Rekomendasi Strategi. Untuk informasi selengkapnya tentang membuat token akses pribadi dengan lingkup repo, lihat Membuat token akses pribadi di GitHubDokumen.

  Untuk menganalisis repositori.NET untuk Porting Assistant untuk rekomendasi .NET, Anda harus menyediakan mesin Windows yang diatur dengan Porting Assistant untuk alat penilaian porting .NET. Untuk informasi selengkapnya, lihat Memulai Porting Assistant untuk.NET di Porting Assistant for .NET User Guide.
- Untuk mengaktifkan Rekomendasi Strategi untuk analisis basis data, Anda harus memasukkan kredensialnya. AWS Secrets Manager Untuk informasi selengkapnya, lihat Analisis basis data Rekomendasi Strategi.
- Anda harus menggunakan AWS Application Discovery Service untuk mengumpulkan data tentang server dan aplikasi Anda di AWS Migration Hub konsol sebelum menggunakan Rekomendasi Strategi. Anda dapat menggunakan salah satu metode berikut untuk mengumpulkan data.
  - Impor Hub Migrasi — Dengan impor Hub Migrasi, Anda dapat mengimpor informasi tentang server dan aplikasi lokal ke Hub Migrasi. Untuk informasi selengkapnya, lihat Impor Hub Migrasi di Panduan Pengguna Application Discovery Service.
  - AWS Application Discovery Service Agentless Collector - Agentless Collector adalah alat VMware yang mengumpulkan informasi tentang mesin virtual VMware (VM). Untuk informasi selengkapnya, lihat Agentless Collector di Panduan Pengguna Application Discovery Service.
  - AWS Agen Penemuan Aplikasi — Agen Penemuan adalah AWS perangkat lunak yang Anda instal di server lokal dan VM untuk menangkap informasi sistem dan detail koneksi jaringan antar sistem. Untuk informasi selengkapnya, lihat Agen Penemuan AWS Aplikasi di Panduan Pengguna Application Discovery Service.
- Pengumpul data Rekomendasi Strategi - Jika server Anda di-host di VMware vCenter, dan Anda memberikan akses, Rekomendasi Strategi dapat secara otomatis mengambil inventaris server

Anda. Konsol Rekomendasi Strategi akan menggunakan informasi yang dikumpulkan untuk membantu penilaian.

> **Note**
>
> Untuk memverifikasi bahwa impor Hub Migrasi berhasil diselesaikan, di panel navigasi konsol Migration Hub, di bawah Temukan, pilih Server. Semua server yang diimpor harus terdaftar.



Langkah 1: Unduh kolektor Rekomendasi Strategi

Rekomendasi Strategi Migrasi Hub Pengumpul data aplikasi adalah alat virtual yang dapat Anda instal di lingkungan VMware lokal Anda. Pengumpul data aplikasi Rekomendasi Strategi juga tersedia sebagai Amazon Machine Image (AMI). Jika Anda ingin menggunakan kolektor versi AMI untuk menilai AWS aplikasi atau karena alasan lain, Anda tidak perlu mengunduh kolektor. Anda dapat melewati bagian ini dan pergi keMenerapkan kolektor Rekomendasi Strategi di instans Amazon EC2.

Bagian ini menjelaskan cara mengunduh file kolektor Open Virtualization Archive (OVA) yang Anda gunakan untuk menyebarkan kolektor sebagai mesin virtual (VM) di lingkungan VMware Anda.

Untuk mengunduh file OVA kolektor

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi.
3. Pada halaman Rekomendasi Strategi Hub Migrasi, pilih Unduh pengumpul data.
4. Secara opsional, Anda dapat memilih Unduh template impor jika Anda ingin mengimpor data aplikasi. Untuk informasi selengkapnya tentang mengimpor data, lihatMengimpor data ke Rekomendasi Strategi.

5. Klik tombol Dapatkan rekomendasi dan pilih Setuju untuk mengizinkan Migration Hub membuat peran terkait layanan (SLR) di akun Anda. Saat menyiapkan Rekomendasi Strategi untuk pertama kalinya, Anda harus membuat SLR. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Rekomendasi Strategi.

Langkah 2: Menyebarkan kolektor Rekomendasi Strategi

Bagian ini menjelaskan cara menyebarkan pengumpul data aplikasi Rekomendasi Strategi. Pengumpul data aplikasi adalah pengumpul data tanpa agen yang mengidentifikasi aplikasi yang berjalan di server Anda, melakukan analisis kode sumber, dan menganalisis database Anda.

Ada dua cara untuk menyebarkan kolektor:

- Menyebarkan sebagai mesin virtual (VM) di VMware vCenter Server Anda. Untuk informasi selengkapnya, lihat Menyebarkan kolektor Rekomendasi Strategi di vCenter.
- Jika Anda memiliki AWS aplikasi yang ingin Anda nilai, Anda dapat menggunakan kolektor Rekomendasi Strategi Amazon Machine Image (AMI). Untuk informasi selengkapnya, lihat Menerapkan kolektor Rekomendasi Strategi di instans Amazon EC2.

Menyebarkan kolektor Rekomendasi Strategi di vCenter

Rekomendasi Strategi Migrasi Hub Pengumpul data aplikasi adalah alat virtual yang dapat Anda instal di lingkungan VMware lokal Anda. Bagian ini menjelaskan cara menyebarkan file kolektor Open Virtualization Archive (OVA) sebagai mesin virtual (VM) di lingkungan VMware Anda.

Prosedur berikut menjelaskan cara menyebarkan kolektor Rekomendasi Strategi di lingkungan VMware vCenter Server Anda.

Untuk menyebarkan kolektor di vCenter

1. Masuk ke vCenter sebagai administrator VMware.
2. Menyebarkan file OVA yang Anda unduh di Langkah 1. File OVA mencakup kolektor dan CLI yang dapat digunakan untuk mengakses API Rekomendasi Strategi.

   Anda juga dapat mengunduh file OVA dari tautan berikut:

   https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova

Kami merekomendasikan spesifikasi berikut untuk VM.

Rekomendasi Strategi spesifikasi VM kolektor

- RAM — minimal 8 GB
- CPU — setidaknya 4

> **Note**
>
> Untuk memastikan bahwa Anda menggunakan kolektor versi terbaru dengan semua fitur baru dan perbaikan bug, tingkatkan kolektor setelah Anda menyebarkan file OVA kolektor. Untuk petunjuk tentang cara meningkatkan, lihatMeningkatkan kolektor Rekomendasi Strategi.

Menerapkan kolektor Rekomendasi Strategi di instans Amazon EC2

Jika Anda memiliki AWS aplikasi yang ingin Anda nilai, Anda dapat menggunakan pengumpul data aplikasi Rekomendasi Strategi Amazon Machine Image (AMI).

Prosedur berikut menjelaskan cara meluncurkan instans Amazon EC2 dari kolektor AMI.

Untuk menyebarkan kolektor instans Amazon EC2

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di bilah navigasi di bagian atas layar, Wilayah saat ini ditampilkan (misalnya, AS Timur (Ohio)). Pilih Wilayah yang sesuai dengan kebutuhan Anda dari Wilayah yang digunakan Rekomendasi Strategi. Untuk daftar Wilayah ini, lihat titik akhir Rekomendasi Strategi di. Referensi Umum AWS
3. Di panel navigasi, di bawah Gambar pilih AMI.
4. Pilih gambar Publik dari dropdown Dimiliki oleh saya.
5. Pilih bilah pencarian dan pilih Nama AMI dari menu.
6. Masukkan nama AWSMHubApplicationDataCollector.
7. Untuk memastikan bahwa AMI berasal dari sumber yang aman, verifikasi bahwa pemilik akun adalah 703163444405.
8. Untuk meluncurkan instance dari AMI ini, pilih, lalu pilih Launch. Untuk informasi selengkapnya tentang meluncurkan instance menggunakan konsol, lihat Meluncurkan instans Anda dari AMI di Panduan Pengguna Amazon EC2.

Kami merekomendasikan spesifikasi berikut untuk instans Amazon EC2.

Rekomendasi Strategi kolektor spesifikasi instans Amazon EC2

- RAM — Minimal 8 GB
- CPU — Setidaknya 4

Rekomendasi Strategi AMI mencakup kolektor dan CLI yang dapat digunakan untuk mengakses API Rekomendasi Strategi.

> **Note**
>
> Untuk memastikan bahwa Anda menggunakan kolektor versi terbaru dengan semua fitur baru dan perbaikan bug, tingkatkan kolektor setelah Anda menggunakan kolektor Rekomendasi Strategi sebagai instans Amazon EC2. Untuk petunjuk tentang cara meningkatkan, lihatMeningkatkan kolektor Rekomendasi Strategi.

Langkah 3: Masuk ke kolektor Rekomendasi Strategi

Bagian ini menjelaskan cara masuk ke pengumpul data aplikasi Rekomendasi Strategi Hub Migrasi yang digunakan. Bagaimana Anda masuk ke kolektor tergantung pada bagaimana Anda menggunakannya.

- Masuk ke kolektor yang digunakan di lingkungan berbasis vCenter
- Masuk ke kolektor yang digunakan sebagai instans Amazon EC2

Masuk ke kolektor yang digunakan di lingkungan berbasis vCenter

Untuk masuk ke kolektor Rekomendasi Strategi yang digunakan di lingkungan berbasis vCenter

1. Gunakan perintah berikut untuk terhubung ke kolektor menggunakan klien SSH.

   ```
   ssh ec2-user@CollectorIPAddress
   ```

2. Saat diminta kata sandi, masukkan kata sandi default aq1 @WSde3. Anda harus mengubah kata sandi saat pertama kali masuk.

Masuk ke kolektor yang digunakan sebagai instans Amazon EC2

Untuk masuk ke kolektor Rekomendasi Strategi yang digunakan sebagai instans Amazon EC2

- Gunakan perintah berikut untuk terhubung ke kolektor menggunakan klien SSH.

  ```
  ssh -i "Keyname.pem" ec2-user@CollectorIPAddress
  ```

  KeyName.pem adalah kunci pribadi yang dihasilkan saat Anda meluncurkan instans Amazon EC2 dari kolektor AMI.

Langkah 4: Siapkan kolektor Rekomendasi Strategi

Bagian ini menjelaskan cara menggunakan baris perintah`collector setup`perintah untuk mengonfigurasi pengumpul data aplikasi Rekomendasi Strategi Hub Migrasi. Konfigurasi ini disimpan secara lokal.

Sebelum Anda dapat menggunakan`collector setup`perintah, Anda harus membuat sesi bash shell di wadah kolektor Docker menggunakan yang berikut`docker exec`perintah.

```
docker exec -it application-data-collector bash
```

The`collector setup`perintah menjalankan semua perintah berikut secara berurutan tetapi Anda dapat menjalankannya satu per satu:

- `collector setup --aws-configurations`— MengaturAWSkonfigurasi.
- `collector setup --vcenter-configurations`— Mengatur konfigurasi vCenter.

> **Note**
>
> Pengaturan konfigurasi vCenter hanya tersedia jika kolektor di-host di vCenter. Namun, Anda dapat memaksa pengaturan konfigurasi vCenter dengan menggunakan perintah`collector setup --vcenter-configurations`.

- `collector setup --remote-server-configurations`— Mengatur konfigurasi server jarak jauh.
- `collector setup --version-control-configurations`— Mengatur konfigurasi kontrol versi.

Untuk mengatur semua konfigurasi kolektor pada saat yang sama

1. Masukkan perintah berikut.

```
collector setup
```

2. Masukkan informasi untukAWSkonfigurasi seperti yang dijelaskan dalamMengaturAWSsusunan.
3. Masukkan informasi untuk konfigurasi vCenter seperti yang dijelaskan dalamSiapkan konfigurasi vCenter.
4. Masukkan informasi untuk konfigurasi server jarak jauh seperti yang dijelaskan dalamSiapkan konfigurasi server jarak jauh.
5. Masukkan informasi untuk konfigurasi kontrol versi seperti yang dijelaskan dalamSiapkan konfigurasi kontrol versi.
6. Siapkan server Windows dan Linux Anda untuk pengumpulan data pengumpul dengan mengikuti petunjuk diSiapkan server Windows dan Linux jarak jauh Anda untuk pengumpulan data.

MengaturAWSsusunan

Untuk mengaturAWSkonfigurasi, saat menggunakan`collector setup`perintah atau`collector setup --aws-configurations`perintah.

1. MasukYuntuk ya untukSudahkah Anda mengatur izin IAM...pertanyaan. Anda mengatur izin ini saat Anda membuat pengguna untuk mengakses kolektor menggunakan`AWSMigrationHubStrategyCollector`kebijakan terkelola mengikuti langkah-langkah diRekomendasi Strategi pengguna dan peran.
2. Masukkan kunci akses dan kunci rahasia Anda dariAWSakun yang memiliki pengguna yang Anda buat untuk mengakses kolektor mengikuti langkah-langkahRekomendasi Strategi pengguna dan peran.
3. Masukkan Wilayah, misalnya,`us-west-2`. Pilih Wilayah yang sesuai dengan kebutuhan Anda dari Wilayah yang digunakan Rekomendasi Strategi. Untuk daftar Wilayah ini, lihatTitik akhir Rekomendasi StrategidiReferensi Umum AWS.
4. MasukYuntuk ya untukUnggah metrik terkait kolektor ke layanan strategi hub migrasi?pertanyaan. Informasi metrik membantuAWSmemberi Anda dukungan yang tepat.
5. MasukYuntuk ya untukUnggah log terkait kolektor ke layanan strategi hub migrasi?pertanyaan. Informasi dari log membantuAWSmemberi Anda dukungan yang tepat.

Contoh berikut menunjukkan apa yang ditampilkan, termasuk entri contoh untukAWSkonfigurasi.

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
 collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
 will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

Siapkan konfigurasi vCenter

Untuk mengatur konfigurasi vCenter, saat menggunakan`collector setup`perintah atau`collector setup --vcenter-configuration`perintah:

1. MasukYuntuk ya untukApakah Anda ingin mengautentikasi menggunakan kredenal VMware vCenterpertanyaan, jika Anda ingin mengautentikasi menggunakan kredenal VMware vCenter.

   > **Note**
   >
   > Otentikasi menggunakan kredensi VMware vCenter mengharuskan alat VMware diinstal pada server target.

   MasukkanUrl Host, yang dapat berupa alamat IP vCenter atau URL. Kemudian, masukkanNama PenggunadanKata Sandiuntuk VMware vCenter.
2. MasukYuntuk ya untukApakah Anda memiliki mesin Windows yang dikelola oleh VMware vCenterpertanyaan, jika Anda ingin mengkonfigurasi server Windows.

MasukkanNama PenggunadanKata Sandiuntuk Windows.

> **Note**
>
> Jika Windows Remote Server milik domain Active Directory, Anda harus memasukkan nama pengguna sebagai*nama-domain**nama pengguna*saat menggunakan CLI untuk menyediakan konfigurasi server jarak jauh. Misalnya, jika nama domain Anda adalah exampledomain dan nama pengguna Anda adalah Administrator, maka nama pengguna yang Anda masukkan di CLI adalahexampledomain\ Administrator.

3. MasukYuntuk ya untukPengaturan untuk Linux menggunakan VMware vCenterpertanyaan, jika Anda ingin mengkonfigurasi server Linux.

   MasukkanNama PenggunadanKata Sandiuntuk Linux.

4. MasukYuntuk ya untukApakah Anda ingin mengatur kredensional untuk server di luar vCenter menggunakan NTLM untuk WindowsdanBerbasis SSH/Cert untuk Linuxpertanyaan, jika Anda ingin mengatur kredensi server jarak jauh untuk server di luar vCenter.
5. UntukApakah Anda ingin menggunakan kredenal Windows yang sama yang digunakan selama pengaturan vCenterpertanyaan, masukkanYuntuk ya jika kredensil untuk mesin Windows yang dikelola di luar vCenter sama dengan kredensil yang diberikan saat mengkonfigurasi kredensil untuk mesin Windows vCenter. Jika tidak, masukkanNuntuk tidak.

   Jika Anda menjawabYuntuk ya, pertanyaan-pertanyaan berikut diajukan.

   a. MasukYuntuk ya untukApakah Anda setuju dengan kolektor yang menerima dan menyimpan sertifikat server secara lokal atas nama Anda selama interaksi pertama dengan server windows?pertanyaan.

   b. Masuk1untukMasukkan opsi Andapertanyaan, jika Anda ingin mengkonfigurasi untuk otentikasi SSH.

      Jika Anda memilih untuk menggunakan otentikasi SSH, Anda harus menyalin kredensi kunci yang dihasilkan ke server Linux Anda. Untuk informasi selengkapnya, lihat Mengatur otentikasi berbasis kunci di server Linux.

Contoh berikut menunjukkan apa yang ditampilkan, termasuk entri contoh untuk konfigurasi VMware vCenter.

```
Your Linux remote server configurations are saved successfully.
collector setup –vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
 installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for Windows (Domain\User): username
Password for Windows: password
Reenter password for Windows: password
Successfully stored windows credentials...
You can verify your setup for vCenter windows machines is correct with "collector diag-
check"
Do you have Linux machines managed by VMWare vCenter? [Y/N]: y
Username for Linux: username
Password for Linux: password
Reenter password for Linux: password
Successfully stored linux credentials...
You can verify your setup for vCenter linux machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using NTLM for
 windows and SSH/Cert based for Linux? [Y/N]: y
Setting up target server for remote execution:
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: y
Successfully stored windows server credentials...
```

```
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
You can verify your setup for remote windows machines is correct with "collector diag-
check"
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y
Generating SSH key on this machine...
Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
You can verify your setup for remote linux machines is correct with "collector diag-
check
```

Siapkan konfigurasi server jarak jauh

Untuk mengatur konfigurasi server jarak jauh, saat menggunakan`collector setup`perintah atau`collector setup --remote-server-configuration`perintah:

1. MasukYuntuk ya untukApakah Anda ingin mengatur kredensil untuk server yang tidak dikelola oleh vCenter menggunakan NLTM untuk Windowspertanyaan, jika Anda ingin mengkonfigurasi server Windows.

   MasukkanNama PenggunadanKata Sandiuntuk WinRM.

   > **Note**
   >
   > Jika Windows Remote Server milik domain Active Directory, Anda harus memasukkan nama pengguna sebagai*`nama-domain`**`nama pengguna`*saat menggunakan CLI untuk menyediakan konfigurasi server jarak jauh. Misalnya, jika nama domain Anda adalah

exampledomain dan nama pengguna Anda adalah Administrator, maka nama pengguna yang Anda masukkan di CLI adalahexampledomain\ Administrator.

MasukYuntuk ya untukApakah Anda setuju dengan kolektor yang menerima dan menyimpan sertifikat server secara lokal atas nama Anda selama interaksi pertama dengan server windows?pertanyaan. Sertifikat Windows Server disimpan dalam direktori`/opt/amazon/application-data-collector/remote-auth/windows/certs`.

Anda harus menyalin kredensi server yang dihasilkan ke server Windows Anda. Untuk informasi selengkapnya, lihat Siapkan konfigurasi server jarak jauh di server Windows.

2. MasukYuntuk ya untukPengaturan untuk Linux menggunakan SSH atau Certpertanyaan, jika Anda ingin mengkonfigurasi server Linux.
3. Masuk1untukMasukkan opsi Andapertanyaan, jika Anda ingin mengkonfigurasi untuk otentikasi berbasis kunci SSH.

   Jika Anda memilih untuk menggunakan otentikasi SSH, Anda harus menyalin kredensi kunci yang dihasilkan ke server Linux Anda. Untuk informasi selengkapnya, lihat Mengatur otentikasi berbasis kunci di server Linux.
4. Masuk2untukMasukkan opsi Andapertanyaan, jika Anda ingin mengonfigurasi otentikasi berbasis sertifikat.

   Untuk informasi tentang menyiapkan otentikasi berbasis sertifikat, lihatMenyiapkan otentikasi berbasis sertifikat di server Linux.

Contoh berikut menunjukkan apa yang ditampilkan, termasuk entri contoh untuk konfigurasi server jarak jauh.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
 in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
```

```
Are you okay with collector accepting and locally storing server certificates on your
 behalf during first interaction with windows servers? These certificates will be used
 by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
 based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
 file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Siapkan konfigurasi kontrol versi

Untuk mengatur konfigurasi kontrol versi, saat menggunakan`collector setup`perintah atau`collector setup --version-control-configurations`perintah:

1. MasukYuntuk ya untukMengatur analisis kode sumber?pertanyaan.
2. Masuk1untukMasukkan opsi Andapertanyaan, jika Anda ingin mengkonfigurasi titik akhir server Git.

   Masukgithub.comuntukTitik akhir server GIT:.
3. Masuk2untukMasukkan opsi Andapertanyaan, jika Anda ingin mengkonfigurasi GitHubServer Perusahaan.

   Masukkan titik akhir perusahaan tanpa https://, sebagai berikut:Titik akhir server GIT: *git-enterprise-endpoint*
4. Masukkan Git Anda*nama pengguna*dan akses pribadi*token*.

5. MasukYuntuk ya untukApakah Anda memiliki repositori csharp yang harus dianalisis pada mesin windows?pertanyaan, jika Anda ingin menganalisis kode C #.

   > **Note**
   >
   > Untuk menganalisis repositori.NET untuk Porting Assistant untuk rekomendasi .NET, Anda harus menyediakan mesin Windows yang diatur dengan Porting Assistant for .NET porting assessment tool. Untuk informasi lebih lanjut, lihatMemulai Porting Assistant untuk.NETdiAsisten Porting untuk Panduan Pengguna .NET.

6. UntukApakah Anda ingin menggunakan kembali kredensi windows yang ada di mesin ini?pertanyaan. MasukYuntuk ya, jika mesin Windows untuk analisis kode sumber C# menggunakan kredensil yang sama dengan kredensil yang sebelumnya disediakan sebagai bagian dari pengaturan`--remote-server-configuration`satau`--vcenter-configurations`.

   MasukNuntuk tidak, jika Anda ingin memasukkan kredensitas baru.

7. Untuk menggunakanMesin VMware vCenter Windowskredensi, masukkan1untukPilih salah satu opsi berikut untuk kredensi windows.

8. Masukkan alamat IP untuk mesin Windows.

Contoh berikut menunjukkan apa yang ditampilkan, termasuk entri contoh untuk konfigurasi kontrol versi.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/
N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
```

```
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

Siapkan server Windows dan Linux jarak jauh Anda untuk pengumpulan data

> **Note**
>
> Langkah ini tidak diperlukan jika Anda mengatur pengumpul data aplikasi Rekomendasi Strategi menggunakan kredensi vCenter.

Setelah Anda mengatur konfigurasi server jarak jauh Anda, jika Anda menggunakan`collector setup command`data`collector setup --remote-server-configuration`perintah, Anda harus menyiapkan server jarak jauh Anda sehingga pengumpul data aplikasi Rekomendasi Strategi dapat mengumpulkan data dari mereka.

> **Note**
>
> Anda harus memastikan bahwa server dapat dijangkau menggunakan alamat IP pribadi mereka. Untuk petunjuk lebih lanjut tentang cara mengatur lingkungan melalui virtual private cloud (VPC) di AWS untuk lari jarak jauh, lihat Panduan Pengguna Amazon Virtual Private Cloud.

Untuk menyiapkan server Linux jarak jauh Anda, lihat Siapkan server Linux jarak jauh.

Untuk menyiapkan server Windows jarak jauh Anda, lihat Siapkan konfigurasi server jarak jauh di server Windows.

Siapkan server Linux jarak jauh

Mengatur otentikasi berbasis kunci di server Linux

Jika Anda memilih untuk mengatur otentikasi berbasis kunci SSH untuk Linux saat mengonfigurasi konfigurasi server jarak jauh, Anda harus melakukan langkah-langkah berikut untuk mengatur otentikasi berbasis kunci di server Anda sehingga data dapat dikumpulkan oleh pengumpul data aplikasi Rekomendasi Strategi.

Untuk mengatur otentikasi berbasis kunci di server Linux Anda

1. Salin kunci publik yang dihasilkan dengan namaid_rsa_assesment.pubdari folder berikut dalam wadah:

   /opt/amazon/application-data-collector/remote-auth/linux/kunci.
2. Tambahkan kunci publik yang disalin di`$HOME/.ssh/authorized_keys`file untuk semua mesin jarak jauh. Jika tidak ada file yang tersedia, buat dengan menggunakan`touch`atau`vim`perintah.
3. Pastikan bahwa folder rumah di server jarak jauh memiliki tingkat izin`755`atau kurang. Jika itu`777`, itu tidak akan berhasil. Anda dapat menggunakan`chmod`perintah untuk membatasi izin.

Menyiapkan otentikasi berbasis sertifikat di server Linux

Jika Anda memilih untuk menyiapkan otentikasi berbasis sertifikat untuk Linux saat mengonfigurasi konfigurasi server jarak jauh, Anda harus melakukan langkah-langkah berikut agar data dapat dikumpulkan oleh pengumpul data aplikasi Rekomendasi Strategi.

Kami merekomendasikan opsi ini jika Anda sudah menyiapkan Certificate Authority (CA) untuk server aplikasi Anda.

Untuk mengatur otentikasi berbasis sertifikat di server Linux Anda

1. Salin nama pengguna yang berfungsi dengan semua server jarak jauh Anda.
2. Salin kunci publik kolektor ke CA.

   Kunci publik untuk kolektor dapat ditemukan di lokasi berikut:

   /opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assesment.pub

   Kunci publik ini harus ditambahkan ke CA Anda untuk menghasilkan sertifikat.

3. Salin sertifikat yang dihasilkan pada langkah sebelumnya ke lokasi berikut di kolektor:

   /opt/amazon/application-data-collector/remote-auth/linux/kunci

   Nama sertifikat harusid_rsa_assesment-cert.pub.
4. Berikan nama file sertifikat selama langkah penyiapan.

Siapkan konfigurasi server jarak jauh di server Windows

Jika Anda memilih untuk mengatur Windows saat mengonfigurasi konfigurasi server jarak jauh dalam pengaturan kolektor, Anda harus melakukan langkah-langkah berikut sehingga data dapat dikumpulkan oleh Rekomendasi Strategi.

> Untuk memahami lebih lanjut tentang PowerShell script yang dijalankan di server jauh, baca catatan ini.
>
> Skrip memungkinkan PowerShell remote dan menonaktifkan semua metode otentikasi selain negosiasi. Ini digunakan untuk Windows NT LAN Manager (NTLM) dan menetapkan”AllowUnencrypted“Protokol WSMan ke false untuk memastikan bahwa pendengar yang baru dibuat hanya menerima lalu lintas terenkripsi. Menggunakan skrip yang disediakan Microsoft,`New-SelfSignedCertificateEx.ps1`, itu menciptakan sertifikat yang ditandatangani sendiri.
> Setiap Instans WSMan yang memiliki pendengar HTTP akan dihapus bersama dengan pendengar HTTPS yang ada. Kemudian, itu membuat pendengar HTTPS baru. Ini juga menciptakan aturan firewall masuk untuk port TCP 5986. Pada langkah terakhir, layanan WinRM dimulai ulang.

Untuk mengatur pengumpulan data melalui koneksi jarak jauh di server Windows 2008

1. Gunakan perintah berikut untuk memeriksa versi PowerShell diinstal pada server Anda.

   ```
   $PSVersionTable
   ```
2. Jika PowerShell versi tidak 5.1, kemudian men-download dan menginstal WMF 5.1 dengan mengikuti petunjuk diInstal dan Konfigurasikan WMF 5.1dalam dokumentasi Microsoft.
3. Gunakan perintah berikut di baru PowerShell jendela untuk memastikan bahwa PowerShell 5.1 diinstal.

```
$PSVersionTable
```

4. Ikuti serangkaian langkah berikutnya, yang menjelaskan cara mengatur pengumpulan data melalui koneksi jarak jauh pada Windows 2012 dan di atasnya.

Untuk mengatur pengumpulan data melalui koneksi jarak jauh pada Windows 2012 dan server yang lebih baru

1. Unduh skrip pengaturan dari URL berikut:

   https://application-data-collector-release. s3.us-west-2.amazonaws.com /scripts/WinrmSetup.ps1

2. Unduh`New-SelfSignedCertificateEx.ps1`dari URL berikut dan tempel skrip ke folder yang sama tempat Anda mengunduh`WinRMSetup.ps1`:

   https://github.com/Azure/azure-libraries-for-net/Blob/master/sampel/aset/baru-SelfSignedCertificateEx.ps1

3. Untuk menyelesaikan pengaturan, jalankan yang diunduh PowerShell skrip di semua server aplikasi.

   ```
   .\WinRMSetup.ps1
   ```

> **Note**
>
> Jika Windows Remote Management (WinRM) tidak diatur dengan benar di Windows Remote Server, upaya untuk mengumpulkan data dari server itu akan gagal. Jika ini terjadi, Anda harus menghapus sertifikat yang sesuai dengan server tersebut dari lokasi berikut pada wadah:
> /opt/amazon/application-data-collector/remote-auth/windows/certs/***ads-server-id***.cer
> Setelah Anda menghapus sertifikat, tunggu proses pengumpulan data dicoba lagi.

Verifikasi bahwa kolektor dan server Anda disiapkan untuk pengumpulan data

Verifikasi bahwa kolektor dan server Anda diatur dengan benar untuk pengumpulan data dengan menggunakan perintah berikut.

```
collector diag-check
```

Perintah ini melakukan serangkaian pemeriksaan diagnostik pada konfigurasi server Anda dan memberikan masukan pada pemeriksaan yang gagal.

Saat Anda menggunakan perintah di-amodus, Anda mendapatkan output dalamDiagnosticCheckResult.txtberkas setelah pemeriksaan selesai.

```
collector diag-check -a
```

Anda dapat melakukan pemeriksaan diagnostik pada konfigurasi server dari satu server dengan alamat IP server tersebut.

Contoh berikut menunjukkan output dari pengaturan yang berhasil.

Server Linux

```
           Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Linux Bash installation...
Linux Bash installation check succeeded
-------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Peladen Windows

```
           Windows PowerShell Version Check succeeded
Provide your test server IP address: IP address
-------------------------------------------------------------
Start checking connectivity & credentials...
Connectivity and Credential Checks succeeded
-------------------------------------------------------------
Start checking permissions...
Permission Check succeeded
-------------------------------------------------------------
Start checking OS version...
OS version check succeeded
-------------------------------------------------------------
Start checking Windows architecture type...
Windows Architecture Type Check succeeded
-------------------------------------------------------------
All diagnostic checks complete successfully.
This server is correctly set up and ready for data collection.
```

Contoh berikut menunjukkan pesan kesalahan yang ditampilkan ketika kredensi server jarak jauh Anda salah.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.
Ensure that your credentials are accurate and the server is configured correctly.
Use the following command to reset incorrect credentials.
collector setup –remote-server-configurations
```

Langkah 5: Gunakan Rekomendasi Strategi di konsol Migration Hub untuk mendapatkan rekomendasi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi di konsol Migration Hub untuk mendapatkan rekomendasi migrasi untuk pertama kalinya.

Untuk mendapatkan rekomendasi

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi.
3. Pada halaman Rekomendasi Strategi Hub Migrasi, pilih Dapatkan rekomendasi.
4. Pilih Setuju jika Anda setuju untuk mengizinkan Migration Hub membuat peran terkait layanan (SLR) di akun Anda. Untuk informasi lebih lanjut tentang SLR, lihatMenggunakan peran terkait layanan untuk Rekomendasi Strategi.
5. Konfigurasikan sumber data

    a. Pada halaman Konfigurasi sumber data, Anda harus memilih sumber server Anda untuk dianalisis dari opsi berikut:

        i. Pengumpul data aplikasi Rekomendasi Strategi — Anda dapat menggunakan kolektor Rekomendasi Strategi untuk mengambil informasi tentang VM yang dihosting di VMware vCenter secara otomatis. Dengan menggunakan opsi ini, Anda tidak perlu melakukan pengaturan tambahan.

        ii. Impor manual - Jika Anda ingin membawa data tentang server dan aplikasi Anda secara independen, Anda dapat menggunakan templat impor Rekomendasi Strategi. Template impor adalah file JSON di mana Anda dapat mengisi informasi yang tersedia untuk VM Anda.

        iii. Application Discovery Service — Anda dapat menggunakan Application Discovery Service untuk mengumpulkan informasi tentang aplikasi dan server lokal Anda. Di konsol Migration Hub, di bawah bagian Alat, Anda dapat memilih dari beberapa opsi di bawah Alat Penemuan. Misalnya, Anda dapat memilih Application Discovery Service Agentless Collector, AWSDiscovery Agent, atau Import (untuk file CSV).

    b. Tabel Server mencantumkan semua server yang tersedia berdasarkan pilihan Anda di bagian sumber data.

    c. Di bawah Pengumpul data aplikasi terdaftar, pengumpul data aplikasi yang telah Anda siapkan terdaftar. Jika Anda belum menyiapkan pengumpul data apa pun, Anda dapat mengunduh pengumpul data dan kemudian menerapkannya. Untuk informasi selengkapnya, silakan lihat Langkah 1: Unduh kolektor Rekomendasi Strategi dan Langkah 2: Menyebarkan kolektor Rekomendasi Strategi.

> **Note**
>
> Untuk mendapatkan rekomendasi strategi, Anda harus menyiapkan setidaknya satu pengumpul data aplikasi atau melakukan impor data aplikasi. Jika Anda ingin menambahkan data tingkat aplikasi Anda tanpa menyiapkan kolektor, Anda dapat menggunakan template impor data aplikasi. Anda dapat menambahkan sumber data tambahan nanti.

d. Jika Anda memilih Impor manual, di bawah Detail impor, pilih Tambahkan impor baru.

e. Untuk nama Impor, masukkan nama untuk impor Anda.

f. Untuk URI bucket S3, masukkan URI bucket S3 untuk file JSON impor Anda untuk diunggah.

> **Important**
>
> Nama bucket S3 harus dimulai dengan awalan. **`migrationhub-strategy`**

g. Pilih Selanjutnya.

6. Tentukan preferensi

   a. Pada halaman Tentukan preferensi, atur sasaran bisnis dan preferensi migrasi Anda. Rekomendasi Strategi merekomendasikan strategi optimal untuk memigrasi dan memodernisasi aplikasi dan database Anda berdasarkan preferensi yang Anda tentukan. Anda dapat mengubah preferensi ini di lain waktu.

   b. Pilih Selanjutnya.

7. Tinjau dan kirimkan.

   a. Tinjau sumber data dan preferensi migrasi yang dikonfigurasi.

   b. Jika semuanya terlihat benar, pilih Mulai analisis data. Ini akan melakukan analisis inventaris server dan lingkungan runtime Anda dan binari aplikasi untuk aplikasi Microsoft IIS dan Java Anda.

> **Note**
>
> Status analisis biner tidak ditampilkan di konsol. Ketika analisis selesai, Anda akan melihat tautan ke laporan anti-pola atau pesan yang menunjukkan bahwa analisis tidak berhasil.

Rekomendasi Strategi

Bagian ini menjelaskan cara melihat rekomendasi migrasi dan modernisasi Rekomendasi Strategi untuk server dan aplikasi dalam portofolio migrasi Anda.

Topik

Melihat rekomendasi strategi dalam Rekomendasi Strategi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi di AWS Migration Hub konsol untuk melihat rekomendasi strategi migrasi.

Untuk melihat rekomendasi strategi

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Rekomendasi.
3. Pada halaman Rekomendasi, Anda dapat melihat dan mengekspor rekomendasi ringkasan portofolio Anda dan rekomendasi strategi “R” migrasi terperinci. Anda juga dapat melihat alat dan tujuan migrasi dan modernisasi, serta anti-pola untuk server dan komponen aplikasi Anda.

   Anti-pola adalah daftar masalah yang diketahui ditemukan dalam portofolio Anda yang dikategorikan berdasarkan tingkat keparahan. Anti-pola keparahan tinggi mewakili ketidakcocokan yang perlu diselesaikan, anti-pola tingkat keparahan sedang mewakili peringatan, dan anti-pola tingkat keparahan rendah mewakili masalah informasi. Untuk informasi tentang strategi “R”, lihat Istilah migrasi - 7 Rs dalam glosarium Panduan AWS Preskriptif.

   - Jika terjadi perubahan di pusat data Anda atau jika Anda memperbarui preferensi Anda, kami sarankan untuk menganalisis ulang data Anda. Untuk menganalisis ulang data Anda untuk mendapatkan rekomendasi baru, pilih Analisis ulang data.

Sampai proses analisis ulang selesai, hasil data rekomendasi Anda dapat berupa campuran data sebelumnya dan data baru.

Untuk mengunduh file laporan dengan rekomendasi, Pilih rekomendasi Ekspor.

4. Pada tab Komponen aplikasi, Anda dapat melihat rekomendasi untuk komponen aplikasi dalam portofolio migrasi Anda. Untuk informasi selengkapnya, lihat Rekomendasi Strategi rekomendasi komponen aplikasi.
5. Pada tab Server, Anda dapat melihat rekomendasi untuk server dalam portofolio migrasi Anda. Untuk informasi selengkapnya, lihat Rekomendasi Strategi rekomendasi server.
6. Pada tab Preferensi, Anda dapat mengedit preferensi yang Anda tentukanLangkah 5: Dapatkan rekomendasi. Untuk informasi tentang mengedit preferensi Anda, lihatPreferensi Rekomendasi Strategi.

Rekomendasi Strategi rekomendasi komponen aplikasi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi di konsol Migration Hub untuk melihat dan menganalisis rekomendasi strategi migrasi untuk komponen aplikasi.

Topik

- Bekerja dengan komponen aplikasi dalam Rekomendasi Strategi
- Rekomendasi Strategi analisis kode sumber
- Analisis basis data Rekomendasi Strategi
- Rekomendasi Strategi analisis biner

Bekerja dengan komponen aplikasi dalam Rekomendasi Strategi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi Hub Migrasi di konsol Hub Migrasi untuk melihat dan mengonfigurasi rekomendasi strategi migrasi dan modernisasi.

Topik

- Melihat rekomendasi komponen aplikasi
- Konfigurasikan analisis kode sumber untuk komponen aplikasi
- Konfigurasikan analisis basis data untuk komponen aplikasi

Melihat rekomendasi komponen aplikasi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi di konsol Migration Hub untuk melihat rekomendasi strategi migrasi untuk komponen aplikasi.

Untuk melihat rincian rekomendasi untuk komponen aplikasi

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Rekomendasi.
3. Pada halaman Rekomendasi, pilih tab Komponen aplikasi.
    a. Di bawah ringkasan komponen Aplikasi, adalah ikhtisar dari berbagai jenis komponen aplikasi yang Anda jalankan dalam portofolio server Anda.
    b. Di bawah Komponen aplikasi, Anda akan melihat nama komponen, jenis komponen, dan rekomendasi strategi “R” migrasi. Anda juga dapat melihat tujuan migrasi, serta alat migrasi dan modernisasi yang akan digunakan untuk berbagai komponen aplikasi yang berjalan dalam portofolio server Anda. Untuk informasi tentang strategi “R”, lihat Istilah migrasi - 7 Rs dalam glosarium Panduan AWS Preskriptif.
4. Untuk melihat detail untuk komponen aplikasi, pilih komponen aplikasi dan kemudian pilih Lihat detail.
5. Pada halaman detail komponen aplikasi (halaman dengan nama komponen sebagai judul) di bawah Ringkasan Rekomendasi, Anda dapat melihat Rekomendasi untuk komponen aplikasi. Anda juga dapat melihat Anti-pola yang diidentifikasi. Anti-pola adalah daftar masalah yang diketahui ditemukan dalam portofolio Anda yang dikategorikan berdasarkan tingkat keparahan.
6. Pilih tab Opsi strategi untuk melihat rekomendasi migrasi untuk komponen aplikasi. Anda dapat mengganti strategi yang disarankan dengan memilih strategi yang berbeda dan kemudian memilih Set yang disukai.
7. Bergantung pada jenis komponen aplikasi yang Anda lihat, ada konfigurasi Sumber atau tab konfigurasi Database. Untuk informasi tentang konfigurasi Sumber, lihatKonfigurasikan analisis kode sumber untuk komponen aplikasi. Untuk informasi tentang konfigurasi Database, lihatKonfigurasikan analisis basis data untuk komponen aplikasi.

Konfigurasikan analisis kode sumber untuk komponen aplikasi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi di konsol Migration Hub untuk mengonfigurasi analisis kode sumber untuk komponen aplikasi.

Untuk mengkonfigurasi analisis kode sumber untuk komponen aplikasi

1. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Rekomendasi.
2. Pada halaman Rekomendasi, pilih tab Komponen aplikasi.
3. Dari daftar komponen di bawah Komponen aplikasi, pilih komponen aplikasi dengan tipe komponen java, dotnetframework, atau IIS, lalu pilih Lihat detail.
4. Pada halaman detail komponen aplikasi (halaman dengan nama komponen sebagai judul), pilih tab konfigurasi kode sumber.
5. Di bawah Rincian konfigurasi kode sumber, pilih Analisis kode sumber.
6. Pada halaman kode sumber Analisis, berikan nama repositori, nama cabang, dan nama proyek (jika ada) yang menyimpan kode sumber untuk komponen aplikasi. Pilih jenis kontrol versi kode GitHub sumber yang ingin Anda gunakan, lalu pilih Analisis.

   Setelah analisis selesai, Anda dapat melihat rekomendasi yang diperbarui pada halaman detail komponen aplikasi.

Untuk informasi selengkapnya tentang analisis kode sumber, lihatRekomendasi Strategi analisis kode sumber.

Konfigurasikan analisis basis data untuk komponen aplikasi

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi di konsol Migration Hub untuk mengonfigurasi analisis database untuk komponen aplikasi.

Untuk mengkonfigurasi analisis database untuk komponen aplikasi

1. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Rekomendasi.
2. Pada halaman Rekomendasi, pilih tab Komponen aplikasi.
3. Dari daftar komponen di bawah Komponen aplikasi, pilih komponen aplikasi dengan tipe komponen SQLServer dan kemudian pilih Lihat detail.
4. Pada halaman detail komponen aplikasi (halaman dengan nama komponen sebagai judul), pilih tab konfigurasi Database.

5. Di bawah Detail konfigurasi database, pilih Analisis detail database.
6. Pilih nama rahasia dari menu tarik-turun yang Anda buat di AWS Secrets Manager untuk digunakan untuk kredensyal database, lalu pilih Analyze.

   Setelah analisis selesai, Anda dapat melihat rekomendasi yang diperbarui pada halaman detail komponen aplikasi.

Untuk informasi selengkapnya tentang analisis database dan menyiapkan nama rahasia, lihatAnalisis basis data Rekomendasi Strategi.

Rekomendasi Strategi analisis kode sumber

Rekomendasi Strategi Migration Hub secara otomatis mengidentifikasi aplikasi dalam portofolio Anda dan membuat komponen aplikasi untuknya. Misalnya, jika ada aplikasi Java dalam portofolio Anda, itu diidentifikasi sebagai komponen aplikasi dengan jenis komponen java.

Rekomendasi Strategi menganalisis kode sumber untuk komponen aplikasi jika Anda mengonfigurasinya untuk melakukannya. Untuk informasi tentang mengonfigurasi komponen aplikasi untuk analisis kode sumber, lihatKonfigurasikan analisis kode sumber untuk komponen aplikasi.

Rekomendasi Strategi melakukan analisis kode sumber untuk bahasa pemrograman Java dan C #.

Untuk informasi tentang prasyarat untuk menggunakan analisis kode sumber Rekomendasi Strategi, lihat. Prasyarat untuk Rekomendasi Strategi

Analisis basis data Rekomendasi Strategi

Rekomendasi Strategi secara otomatis mengidentifikasi server database dalam portofolio Anda dan membuat komponen aplikasi untuk mereka. Misalnya, jika ada database SQL Server dalam portofolio Anda, itu diidentifikasi sebagai komponen aplikasi sqlservr.exe.

Rekomendasi Strategi menganalisis database individu dalam komponen aplikasi SQL Server yang diidentifikasi, sqlservr.exe, menggunakan Schema Conversion AWS Tool. Rekomendasi Strategi juga mengidentifikasi ketidakcocokan dalam memigrasikan database ke database AWS seperti Amazon Aurora MySQL Compatible Edition, Amazon Aurora PostgreSQL Compatible Edition, Amazon RDS for MySQL, dan Amazon RDS for PostgreSQL.

Saat ini, analisis basis data Rekomendasi Strategi hanya tersedia untuk SQL Server.

Untuk mengonfigurasi Rekomendasi Strategi untuk menganalisis basis data Anda, Anda harus memberikan kredensyal untuk pengumpul data aplikasi Rekomendasi Strategi untuk terhubung ke database Anda. Untuk melakukan ini, buat AWS rahasia di Secrets Manager di AWS akun Anda.

Untuk informasi tentang izin dan hak istimewa kredensil yang Anda berikan, lihat. Hak istimewa yang diperlukan untuk AWS kredensyal Alat Konversi Skema Untuk informasi tentang membuat rahasia dengan kredensialnya, lihat. Membuat rahasia di Secrets Manager untuk kredensyal database

Setelah Anda mengatur kredensil dan rahasia, Anda dapat mengonfigurasi analisis AWS Schema Conversion Tool di server database. Untuk informasi selengkapnya, lihat Konfigurasikan analisis basis data untuk komponen aplikasi.

Setelah Anda mengonfigurasi analisis database untuk komponen aplikasi, tugas inventaris AWS Schema Conversion Tool dijadwalkan. Setelah tugas ini selesai, Anda akan melihat komponen aplikasi baru yang dibuat untuk setiap database individu di server database tersebut. Misalnya, jika SQL Server Anda memiliki dua database (exampledbs1 dan exampledbs2), komponen aplikasi dibuat untuk masing-masing database dengan nama exampledbs1 dan exampledbs2.

Jika Anda ingin melihat anti-pola dalam memigrasikan setiap database yang diidentifikasi ke AWS database, siapkan analisis untuk setiap database dengan mengikuti langkah-langkahnya. Konfigurasikan analisis basis data untuk komponen aplikasi

Hak istimewa yang diperlukan untuk AWS kredensyal Alat Konversi Skema

Kredensi login yang Anda berikan kepada AWS Secrets Manager hanya kebutuhan `VIEW SERVER STATE` dan hak istimewa. `VIEW ANY DEFINITION` Secara opsional, Anda dapat membuat login baru dengan menggunakan skrip yang tersedia di https://gitlab.aws.dev/dmaf-pub/dmaf/-/blob/master/create_mssql_ro_user.sql.

Anda dapat memberikan nama login dan kata sandi yang Anda inginkan saat membuat login SQL Server.

Membuat rahasia di Secrets Manager untuk kredensyal database

Setelah kredensyal siap untuk pengumpul data aplikasi Rekomendasi Strategi untuk terhubung ke database, buat AWS rahasia di Secrets Manager di AWS akun Anda seperti yang dijelaskan dalam prosedur berikut.

Untuk membuat rahasia dengan AWS Secrets Manager di AWS akun Anda

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol AWS Secrets Manager di https://console.aws.amazon.com/secretsmanager/.
2. Pilih Simpan rahasia baru.
3. Pilih jenis rahasia sebagai Jenis rahasia lainnya.
4. Di bawah pasangan kunci/nilai, masukkan informasi berikut.

   nama pengguna - nama pengguna *Anda*

   Kemudian pilih + Tambahkan baris dan masukkan informasi berikut.

   kata sandi - kata sandi *Anda*
5. Pilih Selanjutnya.
6. Masukkan nama Rahasia sebagai string apa pun dengan awalan migrationhub-strategy -. Misalnya, migrationhub-strategy-one.

   > **Note**
   >
   > Simpan nama rahasia Anda di tempat yang aman untuk digunakan nanti.
7. Pilih Berikutnya, lalu pilih Berikutnya lagi.
8. Pilih Toko.

Anda dapat menggunakan rahasia yang Anda buat untuk kredensi database saat menyiapkan analisis basis data di Rekomendasi Strategi.

Rekomendasi Strategi analisis biner

Rekomendasi Strategi Migrasi Hub secara otomatis mengidentifikasi aplikasi dalam portofolio Anda dan komponen aplikasi yang menjadi miliknya. Misalnya, jika ada aplikasi Java dalam portofolio Anda, Rekomendasi Strategi mengidentifikasinya sebagai komponen aplikasi dengan jenis komponen java. Tanpa Anda mengonfigurasi akses ke kode sumber, Rekomendasi Strategi dapat melakukan analisis biner. dengan memeriksa DLL aplikasi IIS pada Windows atau file JAR aplikasi di Linux dan memberikan laporan anti-pola atau laporan ketidakcocokan. Laporan anti-pola adalah daftar masalah yang diketahui yang ditemukan oleh Rekomendasi Strategi dalam portofolio Anda,

dikategorikan berdasarkan tingkat keparahan. Laporan ketidakcocokan berisi subset anti-pola, yaitu kompatibilitas API, Nuget Package, dan Porting Action.

Rekomendasi Strategi melakukan analisis untuk aplikasi Windows IIS dan Java Tomcat dan Jboss. Jika Anda memiliki aplikasi IIS, Rekomendasi Strategi menghasilkan laporan ketidakcocokan secara default; Anda harus mengonfigurasi akses kode sumber untuk menerima laporan anti-pola lengkap. Jika Anda memiliki aplikasi Java, Rekomendasi Strategi menghasilkan laporan anti-pola lengkap secara default.

Laporan yang tidak kompatibel atau anti-pola ditampilkan setelah analisis selesai. Jika analisis tidak berhasil, Anda dapat mencoba menjalankan analisis kode sumber dengan menyediakan akses kode sumber seperti yang dijelaskan dalamSiapkan konfigurasi kontrol versi.

Rekomendasi Strategi rekomendasi server

Bagian ini menjelaskan cara menggunakan Rekomendasi Strategi Hub Migrasi di konsol Hub Migrasi untuk melihat rekomendasi strategi migrasi untuk server dalam portofolio migrasi Anda.

Untuk melihat rekomendasi untuk server

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Rekomendasi.
3. Pada halaman Rekomendasi, pilih tab Server.

    a. Di bawah ringkasan Server, Anda melihat ikhtisar berbagai jenis server yang Anda jalankan dalam portofolio Anda.

    b. Di bawah Server, Anda melihat detail server dan sistem operasi serta rekomendasi strategi migrasi “R”. Anda juga dapat melihat tujuan migrasi dan jumlah anti-pola yang diidentifikasi di server Anda, yang didasarkan pada rekomendasi. Untuk informasi tentang strategi “R”, lihat Istilah migrasi - 7 Rs dalam glosarium Panduan AWS Preskriptif.
4. Untuk melihat detail rekomendasi mendalam untuk server, pilih server dari daftar, lalu pilih Lihat detail. Anda dapat melihat metadata yang dikumpulkan untuk server, bersama dengan analisis mendalam dan rekomendasi untuk itu, yang didasarkan pada komponen aplikasi yang ditemukan berjalan di server.
5. Pada halaman detail server (halaman dengan nama server sebagai judul), di bawah ringkasan Rekomendasi, Anda dapat melihat ikhtisar rekomendasi Strategi untuk server. Anda juga dapat

melihat Anti-pola yang diidentifikasi. Anti-pola adalah daftar masalah yang diketahui ditemukan dalam portofolio Anda yang dikategorikan berdasarkan tingkat keparahan.

6. Pilih tab Opsi strategi untuk melihat rekomendasi migrasi server. Anda dapat mengganti strategi yang disarankan dengan memilih strategi yang berbeda dan kemudian memilih Set yang disukai.
7. Pilih tab Komponen aplikasi untuk melihat daftar komponen aplikasi yang terkait dengan server.
8. Untuk melihat detail tentang komponen aplikasi, pilih komponen dari daftar dan kemudian pilih Lihat detail. Untuk informasi selengkapnya tentang komponen aplikasi, lihatBekerja dengan komponen aplikasi.

Preferensi Rekomendasi Strategi

Bagian ini menjelaskan cara melihat dan mengedit preferensi Rekomendasi Strategi Hub Migrasi di konsol Hub Migrasi.

Anda memilih preferensi rekomendasi saat pertama kali menyiapkan Rekomendasi Strategi seperti yang dijelaskan dalamLangkah 5: Dapatkan rekomendasi. Anda dapat mengedit preferensi ini.

Untuk mengedit preferensi rekomendasi

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Rekomendasi.
3. Pada halaman Rekomendasi, pilih tab Preferensi.
4. Di bawah tujuan bisnis yang diprioritaskan, Anda dapat menarik dan melepaskan tujuan bisnis untuk mengatur ulang mereka.
5. Pilih preferensi Aplikasi dan preferensi Database yang Anda inginkan, lalu pilih Simpan perubahan.

Jika Anda mengubah preferensi Anda, spanduk ditampilkan untuk mengingatkan Anda untuk memilih Menganalisis ulang data.

Rekomendasi Strategi sumber data

Bagian ini menjelaskan sumber data yang digunakan Rekomendasi Strategi.

Topik

Melihat sumber data Rekomendasi Strategi

Bagian ini menjelaskan cara melihat sumber data Rekomendasi Strategi di AWS Management Console.

Untuk melihat sumber data

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Sumber data.
3. Pada tab Kolektor, Anda dapat melihat pengumpul data aplikasi Rekomendasi Strategi yang Anda siapkan. Untuk informasi lebih lanjut tentang kolektor, lihatRekomendasi Strategi pengumpul data aplikasi.
4. Pada tab Impor, Anda dapat mengimpor data dan melihat impor data Anda. Untuk informasi selengkapnya, lihat Mengimpor data ke Rekomendasi Strategi.
5. Pada tab Alat, Anda dapat mengunduh templat data impor kolektor dan aplikasi.

Rekomendasi Strategi pengumpul data aplikasi

Bagian ini menjelaskan cara menggunakan pengumpul data aplikasi Rekomendasi Strategi.

Untuk informasi tentang mengunduh dan menyiapkan pengumpul data aplikasi, lihatLangkah 1: Unduh kolektor Rekomendasi Strategi.

Topik

Data yang dikumpulkan oleh kolektor Rekomendasi Strategi

Bagian ini menjelaskan jenis data yang dikumpulkan oleh pengumpul data aplikasi Rekomendasi Strategi Hub Migrasi. Pengumpul data aplikasi adalah pengumpul data tanpa agen yang mengidentifikasi aplikasi yang berjalan di server Anda, melakukan analisis kode sumber, dan menganalisis database Anda.

Bidang data	Deskripsi
Jenis OS	Windows atau Linux
Versi OS	Versi spesifik dari OS. Misalnya, Windows Server 2003, RHEL 5.2.
Arsitektur OS	OS 32-bit atau 64-bit
Adalah Server VM	Server adalah VM atau mesin fisik.
Perangkat lunak virtualisasi	Misalnya, vCenter, Hyper-V.
Lokasi	Misalnya, konsol Amazon Elastic Compute Cloud (Amazon EC2), atau lokal.
Adalah DualBoot	Memungkinkan booting ke beberapa OS
Jenis firmware	BIOS, UEFI
Pemuat boot	GRUB, GRUB 2
Jenis tabel partisi	MBR, GPT
Kecepatan CPU	Kecepatan CPU dalam GHz. Misalnya, 2, 4 GHz.
Windows OS data	

Bidang data	Deskripsi
Edisi Windows	Standar, Pusat Data, Perusahaan
Versi kerangka kerja .NET	Versi Framework .NET diinstal.
.NET versi Core	Versi .NET Core diinstal.
Linux data	
Distribusi OS Linux	RHEL, CentOS, SUSE, dan sebagainya.
Versi Kernel	uname -r output, seperti `4.9.217-0.1.ac.205.84.332.metal1.x86_64`
For each disk volume	
Jenis sistem file	FAT32, NTFS, ReFS, ext4, jfs, dan sebagainya.
Ukuran volume disk	Ukuran disk total
Ruang kosong volume disk	Ruang disk kosong
Format gambar disk virtual	vmdk, vhd, vhdx
Jenis disk (Windows)	Dasar, Dinamis
Application level data	
Nama aplikasi	Nama proses yang sedang berjalan. Misalnya, SQLServr.exe, MSdtsservr.exe, dan sebagainya.
Jenis aplikasi	IIS, JBoss, Tomcat, dan sebagainya.
Bahasa pemrograman & versi	C#, Jawa
Versi JDK	Versi JDK diinstal.
Apakah kode sumber tersedia	Jika Anda menyediakan repositori kode sumber, ini menunjukkan bahwa kode sumber tersedia.

Bidang data	Deskripsi
Ukuran bit aplikasi	16-bit, 32-bit, 64-bit
Windows	
Versi Framework .NET yang digunakan oleh aplikasi	Versi DLL framework .NET sedang dimuat saat runtime untuk aplikasi.
.NET versi Core	Versi .NET Core DLL sedang dimuat saat runtime untuk aplikasi.
Menggunakan kerangka WPF?	Menentukan apakah aplikasi berbasis .NET adalah jenis aplikasi WPF atau tidak.
Menggunakan kerangka WCF?	Menentukan apakah aplikasi berbasis .NET adalah jenis aplikasi WCF atau tidak.
Versi ASP.NET	Versi ASP.NET.
Versi IIS	Versi server IIS diinstal pada mesin Windows.
Ukuran bit driver OS aplikasi	32-bit, 64-bit
Penggunaan registri Windows	Memeriksa kunci registri mesin untuk menemukan informasi seperti versi database, versi Java, versi.NET, dan sebagainya.
Semua DLL yang digunakan oleh aplikasi	Mengambil daftar semua DLL yang dimuat saat runtime oleh proses Windows.
PowerShell versi	Memeriksa PowerShell versi yang diinstal pada mesin, yang seharusnya 5.1 atau lebih baru.
Linux	
Jenis kerangka aplikasi	Tomcat, Sepatu Bot Musim Semi, JBoss,, WebLogic WebSphere
Versi kerangka aplikasi	Versi kerangka aplikasi.

Bidang data	Deskripsi
Database	
Jenis basis data	MS SQL, Oracle, MySQL, dan sebagainya.
Versi basis data	Versi database.

Menghapus data Anda dari Rekomendasi Strategi

Agar semua data Anda dihapus dari Rekomendasi Strategi, hubungi AWS Supportdan minta penghapusan data lengkap.

Meningkatkan kolektor Rekomendasi Strategi

Pengumpul data aplikasi Rekomendasi Strategi Hub Migrasi ditingkatkan secara otomatis. Anda dapat menggunakan prosedur berikut untuk meng-upgrade kolektor secara manual, jika diperlukan.

Untuk meng-upgrade kolektor Rekomendasi Strategi

1. Gunakan perintah berikut untuk terhubung ke VM kolektor menggunakan klien SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Ubah ke direktori upgrade di VM kolektor seperti yang ditunjukkan pada contoh berikut.

```
cd  /home/ec2-user/collector/upgrades
```

3. Gunakan perintah berikut untuk menjalankan skrip upgrade.

```
sudo bash application-data-collector-upgrade
```

Mengimpor data ke Rekomendasi Strategi

Sebagai alternatif untuk menggunakan pengumpul data aplikasi, Anda dapat mengimpor informasi tentang aplikasi dan server yang Anda inginkan rekomendasi migrasi dan modernisasi.

Saat Anda mengimpor data, rekomendasinya tidak sedalam saat Anda menggunakan pengumpul data. Misalnya, Anda tidak dapat menggunakan analisis kode sumber pada data yang diimpor.

Bagian ini menjelaskan cara menggunakan templat impor aplikasi untuk mengimpor data ke Rekomendasi Strategi di konsol Migration Hub.

Untuk mengimpor data

1. Menggunakan AWS akun yang Anda buatMenyiapkan Rekomendasi Strategi, masuk ke AWS Management Console dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Strategi, lalu pilih Sumber data.
3. Pilih tab Impor.
4. Pilih Unduh templat impor untuk mengunduh templat impor aplikasi.
5. Isi template dan unggah ke bucket Amazon S3. Pastikan bahwa nama bucket dimulai dengan awalan`migrationhub-strategy`.
6. Kembali ke tab Impor dan kemudian pilih Impor.
7. Masukkan nama untuk impor Anda, masukkan URI objek Amazon S3 untuk templat data yang Anda isi, lalu pilih Mulai impor.

Templat impor Rekomendasi Strategi

Template impor yang Anda download adalah `.json` file seperti yang ditunjukkan pada contoh berikut.

```
{
    "ImportFormatVersion": 1,
    "Resources": [
        {
            "ResourceType": "SERVER",
            "ResourceName": "",
            "ResourceId": "",
            "IpAddress": "",
            "OSDistribution": "",
            "OSType": "",
            "HostName": "",
            "OSVersion": "",
            "CPUArchitecture": ""
        },
        {
            "ResourceType": "PROCESS",
            "ResourceName": "",
```

```
            "ResourceId": "",
            "ApplicationType": "",
            "DotNetFrameworkVersion": "",
            "ApplicationVersion": "",
            "DotNetCoreVersion": "",
            "JdkVersion": "",
            "ProgrammingLanguage": "",
            "DatabaseType": "",
            "DatabaseVersion": "",
            "DatabaseEdition": "",
            "AssociatedServerIds": []
        }
    ]
}
```

Untuk membantu Anda mengisi template impor, nilai yang valid untuk bidang data tercantum dalam tabel berikut.

Bidang yang diperlukan untuk server tercantum dalam tabel berikut.

Nama	Penjelasan	Jenis	Dibutuhkan	Nilai valid
ResourceId	ID unik untuk sumber daya	Tali	Ya	String unik apa pun
ResourceName	Nama sumber daya	Tali	Ya	Semua string
ResourceType	Jenis sumber daya untuk diimpor	Tali	Ya	“Server”, “Proses”
OSDistribusi	Windows, Windows Server, Ubuntu	Tali	Ya	Windows: “PC Windows”, “Server Windows” Linux: “Ubuntu”, “RHEL”, “Amazon Linux”, “DEBIAN”, “SLES”, “CENT_OS” , “ORACLE_LINUX”, “FEDORA”, “KALI”

Nama	Penjelasan	Jenis	Dibutuhkan	Nilai valid
Ostype	Jenis sistem operasi	Tali	Ya	“Windows”, “Linux”
OSVersion	Versi kernel	Tali	Ya	Lihat versi HTML dari dokumentasi.
CPUArsitektur	Arsitektur CPU	String	Tidak	“32bit”, “64bit”
IpAddress	Alamat IP server	Array	Tidak	Dalam format xxx.xxx.xxx.xxx
MacAddresses	Alamat Mac yang terkait dengan server	Array	Tidak	Dalam format xx:xx:xx:xx:xx:xx
Nama host	Nama tuan rumah	String	Tidak	String apa pun

Bidang yang diperlukan untuk proses tercantum dalam tabel berikut.

Nama	Penjelasan	Jenis	Dibutuhkan	Nilai valid
ResourceId	ID unik untuk sumber daya	Tali	Ya	String unik apa pun
ResourceName	Nama sumber daya	Tali	Ya	Semua string
ResourceType	Jenis sumber daya untuk diimpor	Tali	Ya	“Server”, “Proses”

Nama	Penjelasan	Jenis	Dibutuhkan	Nilai valid
AssociatedServerIds	Daftar ID server tempat proses berjalan.	Tali	Ya	ResourceId Dari "Resource Type“: “SERVER” yang Anda tentukan.
ApplicationType	Jenis aplikasi	Tali	Ya	“Tomcat”, “JBoss”, “Musim Semi”, “IIS”, “Mongo DB”, “DB2", “Maria DB”, “MySQL”, “Oracle”, “SqlServer”, “Sybase”, “PostgreSQLServer” , “Cassandra”, “IBM “, “Oracle “, “Java Generik” WebSphere WebLogic
ApplicationVersion	Versi aplikasi	Tali	Ya	“IIS 1.0", “IIS 2.0", “IIS 3.0", “IIS 4.0", “IIS 5.0", “IIS 6.0", “IIS 7.0", “IIS 7.5", “IIS 8.0", “IIS 8.5", “IIS 10.0"
ProgrammingLanguage	Bahasa pemrograman untuk aplikasi	String	Tidak	“Java”, “CSharp”

Nama	Penjelasan	Jenis	Dibutuhkan	Nilai valid
DotNetFrameworkVersion	Versi .NET Framework jika aplikasi berbasis .NET Framework	String	Tidak	“DotnetFramework 1.0"," DotnetFramework 1.0 SP1", "1.0 SP2"," DotnetFramework 1.0 SP3", "DotnetFramework 1.1"," DotnetFramework DotnetFramework 1.1 SP1", "DotnetFramework2.0"," 2.0 SP1", "DotnetFramework 2.0 SP2"," 3.0", "3.0 SP1"," DotnetFramework 3.0 SP2", "DotnetFramework 3.5"," DotnetFramework DotnetFramework 3.5 SP1", "4.0"," DotnetFramework 4.5", "4.5.1"," DotnetFramework 4.5.2", "DotnetFramework4.5.2"," 4.6", "4.6.1"," 4.6.2", "DotnetFramework 4.7"," DotnetFramework 4.7.1", "4.7.2"," 4.8" DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework DotnetFramework
DotNetCoreVersion	Versi .NET Core jika aplikasi berbasis .NET Core	String	Tidak	“.NET Core 1.0", “.NET Core 1.1", “.NET Core 2.0", “.NET Core 2.1", “.NET Core 2.2", “.NET Core 3.0", “.NET Core 3.1"

Nama	Penjelasan	Jenis	Dibutuhkan	Nilai valid
JdkVersion	Versi JDK, jika aplikasi menggunakan JDK	String	Tidak	“JDK1.0", “JDK2.0", “JDK3.0", ..., “JDK11.0"
DatabaseType	Jenis database	String	Tidak	“SQLServer”, “Oracle”, “Sybase”, “Mongo DB”, “Maria DB”, “Apache Cassandra ”, “MySQL”, “IBM DB2", “PostgreSQLServer”
DatabaseEdition	Edisi database	String	Tidak	
DatabaseVersion	Versi database	String	Tidak	Lihat versi HTML dari dokumentasi.

Menghapus data Anda dari Rekomendasi Strategi

Untuk menghapus semua data Anda dari Rekomendasi Strategi Hub Migrasi, hubungi AWS Support.

Rekomendasi Strategi Keamanan dalam Migration Hub

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menggambarkan ini sebagai keamanan dari cloud dan keamanan di dalam cloud:

- Keamanan dari cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di Cloud AWS Cloud. AWS juga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara berkala efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku pada Rekomendasi Strategi Pusat Migrasi, lihat AWSLayanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan .
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Rekomendasi Strategi. Topik berikut menunjukkan cara mengonfigurasi Rekomendasi Strategi untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Rekomendasi Strategi Anda.

Topik

Perlindungan data dalam Rekomendasi Strategi Migration Hub

Model tanggung jawab AWS bersama model tanggung berlaku untuk perlindungan data dalam Rekomendasi Strategi Hub Migrasi. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk memberikan perlindungan terhadap infrastruktur global yang menjalankan semua

AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk AWS services yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data. Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam AWS services.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Rekomendasi Strategi atau lainnya AWS services menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menyarankan jangan menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi saat tidak aktif

Semua data yang disimpan dalam database Rekomendasi Strategi dienkripsi.

Enkripsi dalam transit

Rekomendasi Strategi komunikasi internetwork mendukung enkripsi TLS 1.2 antara semua komponen dan klien.

Manajemen identitas dan akses untuk Rekomendasi Strategi Migration Hub

AWS Identity and Access Management (IAM) adalah AWS service yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Rekomendasi Strategi. IAM adalah AWS service yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan dalam Rekomendasi Strategi.

Pengguna layanan — Jika Anda menggunakan layanan Rekomendasi Strategi untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Rekomendasi Strategi untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta

izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Rekomendasi Strategi, lihatPemecahan Masalah Identitas dan akses Rekomendasi Strategi Migration Hub.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Rekomendasi Strategi di perusahaan Anda, Anda mungkin memiliki akses penuh ke Rekomendasi Strategi. Tugas Anda adalah menentukan fitur dan sumber daya Rekomendasi Strategi mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Rekomendasi Strategi, lihatBagaimana Rekomendasi Strategi Hub Migrasi bekerja dengan IAM.

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Rekomendasi Strategi. Untuk melihat contoh Kebijakan berbasis identitas Rekomendasi Strategi yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi Migration Hub

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan

metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua AWS services dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS services dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses AWS services dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS services, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa AWS services menggunakan fitur lain AWS services. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama AWS service, dikombinasikan dengan permintaan AWS service untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS services atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke AWS service dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS service Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans

EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana,

dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. AWS services

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Rekomendasi Strategi Hub Migrasi bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Rekomendasi Strategi, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Rekomendasi Strategi.

Fitur IAM yang dapat Anda gunakan dengan Rekomendasi Strategi Migration Hub

Fitur IAM	Dukungan Rekomendasi Strategi
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Tidak
Kunci kondisi kebijakan	Tidak
ACL	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin prinsipal	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan pandangan tingkat tinggi tentang cara kerja Rekomendasi Strategi dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Rekomendasi Strategi

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi

Untuk melihat contoh kebijakan berbasis identitas Rekomendasi Strategi, lihat. Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi Migration Hub

Kebijakan berbasis sumber daya dalam Rekomendasi Strategi

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. AWS services

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Tindakan kebijakan untuk Rekomendasi Strategi

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Rekomendasi Strategi, lihat Tindakan yang Ditentukan oleh Rekomendasi Strategi Hub Migrasi di Referensi Otorisasi Layanan.

Tindakan kebijakan dalam Rekomendasi Strategi menggunakan awalan berikut sebelum tindakan:

```
migrationhub-strategy
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "migrationhub-strategy:action1",
      "migrationhub-strategy:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Rekomendasi Strategi, lihat. Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi Migration Hub

Sumber daya kebijakan untuk Rekomendasi Strategi

Mendukung sumber daya kebijakan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Rekomendasi Strategi dan ARNnya, lihat Sumber Daya yang Ditentukan oleh Rekomendasi Strategi Hub Migrasi di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Rekomendasi Strategi Hub Migrasi.

Untuk melihat contoh kebijakan berbasis identitas Rekomendasi Strategi, lihat. Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi Migration Hub

Kunci kondisi kebijakan untuk Rekomendasi Strategi

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Rekomendasi Strategi, lihat Kunci Kondisi untuk Rekomendasi Strategi Hub Migrasi di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Rekomendasi Strategi Hub Migrasi.

Untuk melihat contoh kebijakan berbasis identitas Rekomendasi Strategi, lihat. Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi Migration Hub

Daftar kontrol akses (ACL) dalam Rekomendasi Strategi

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan Rekomendasi Strategi

Mendukung ABAC (tag dalam kebijakan): Tidak

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal Sementara dengan Rekomendasi Strategi

Mendukung kredensyal sementara: Ya

Beberapa AWS services tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang AWS services bekerja dengan kredensi sementara, lihat AWS services yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensil sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Rekomendasi Strategi

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama AWS service, dikombinasikan dengan permintaan AWS service untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS services atau sumber daya untuk

menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Rekomendasi Strategi

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke AWS service dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Rekomendasi Strategi. Edit peran layanan hanya jika Rekomendasi Strategi memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Rekomendasi Strategi

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. AWS service Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan Rekomendasi Strategi, lihat. Menggunakan peran terkait layanan untuk Rekomendasi Strategi

AWS kebijakan terkelola untuk Rekomendasi Strategi Hub Migrasi

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau saat operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSMigrationHubStrategyConsoleFullAccess

Anda dapat melampirkan kebijakan `AWSMigrationHubStrategyConsoleFullAccess` ke identitas IAM Anda.

`AWSMigrationHubStrategyConsoleFullAccess`Kebijakan ini memberikan pengguna akses penuh ke layanan Rekomendasi Strategi melalui. AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `discovery`— Memberikan akses pengguna untuk mendapatkan ringkasan penemuan di Application Discovery Service.
- `iam`— Memungkinkan peran terkait layanan dibuat untuk pengguna, yang merupakan persyaratan untuk menggunakan Rekomendasi Strategi.
- `migrationhub-strategy`— Memberi pengguna akses penuh ke Rekomendasi Strategi.
- `s3`— Memungkinkan pengguna untuk membuat dan membaca dari bucket S3 yang digunakan oleh Rekomendasi Strategi.
- `secretsmanager`— Memungkinkan pengguna untuk daftar akses rahasia di Secrets Manager.

Untuk melihat izin kebijakan ini, lihat AWSMigrationHubStrategyConsoleFullAccessdi Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AWSMigrationHubStrategyCollector

Anda dapat melampirkan kebijakan `AWSMigrationHubStrategyCollector` ke identitas IAM Anda.

Detail izin

Kebijakan ini mencakup izin berikut.

- `application-transformation`— Memberikan izin untuk mengunggah data log dan metrik untuk operasi transformasi aplikasi dan bekerja dengan penilaian dan rekomendasi kompatibilitas porting.
- `execute-api`— Memungkinkan pengguna mengakses Amazon API Gateway untuk mengunggah log dan metrik ke AWS.
- `migrationhub-strategy`— Memberi pengguna akses untuk mendaftarkan pesan, mengirim pesan, mengunggah data log, dan mengunggah data metrik ke Rekomendasi Strategi.
- `s3`— Memberikan pengguna akses ke daftar bucket dan lokasi mereka. Pengguna juga diberikan akses untuk menulis, mengambil objek dari, menambahkan objek ke, mengembalikan daftar kontrol akses (ACL) dari, membuat, mengakses, mengonfigurasi enkripsi untuk, memodifikasi `PublicAccessBlock` konfigurasi untuk, mengatur status versi untuk, dan membuat atau mengganti konfigurasi siklus hidup untuk bucket S3 yang digunakan oleh Rekomendasi Strategi.
- `secretsmanager`— Memungkinkan pengguna untuk mengakses rahasia di Secrets Manager yang digunakan oleh Rekomendasi Strategi.

Untuk melihat izin kebijakan ini, lihat AWSMigrationHubStrategyCollectordi Panduan Referensi Kebijakan AWS Terkelola.

Rekomendasi Strategi memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Rekomendasi Strategi sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Rekomendasi Strategi.

Perubahan	Deskripsi	Tanggal
AWSMigrationHubStrategyCollector — Permbaruan ke kebijakan yang sudah ada	Kebijakan ini diperbaru i untuk menyertakan tindakan transformasi `PutLogData` `StartPort ingCompatibilityAs sessment` `GetPortin gCompatibilityAsse ssment` ,, `StartPort ingRecommendationA ssessment` dan `GetPortingRecommen dationAssessment` aplikasi untuk memungkinkan layanan transformasi aplikasi mengirim log dan metrik ke layanan. `ListBucket` Dan `GetBucketLocation` ditambahkan untuk Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) untuk mendukung unggahan log dan metrik. `PutLogDat a` Dan juga `PutMetric Data` ditambahkan untuk memungkinkan kolektor Rekomendasi Strategi mengirim log dan metrik ke titik akhir layanan.	April 1, 2024
AWSMigrationHubStrategyCollector – Pembaruan ke kebijakan yang ada	Kebijakan ini diperbaru i dengan `PutLogData` tindakan `PutMetricData` dan tindakan. Tindakan ini	Februari 5, 2024

Perubahan	Deskripsi	Tanggal
	memberikan pengungga han log dan data metrik untuk operasi transformasi aplikasi. Pembaruan ini juga menambahkan ketentuan untuk memastikan bahwa sama dengan izin `aws:Princ ipalAccount` untuk menggunakan Layanan dan AWS Secrets Manager tindakan Amazon Simple Storage yang disertakan. `aws:ResourceAccount`	
AWSMigrationHubStrategyCollector – Pembaruan ke kebijakan yang ada	Kebijakan ini diperbarui dengan API Amazon S3 berikut —`CreateBuc ket` ,,,`PutEncryp tionConfiguration` , `PutBucketPublicAcc essBlock` `PutBucket Policy` `PutBucket Versioning` , dan. `PutLifecycleConfig uration`	15 September 2023
AWSMigrationHubStrategyCollector – Pembaruan ke kebijakan yang ada	Pembaruan kebijakan ini memberikan izin yang memungkinkan analisis kode sumber.	8 Maret 2023

Perubahan	Deskripsi	Tanggal
AWSMigrationHubStrategyConsoleFullAccess – Pembaruan ke kebijakan yang ada	Kebijakan ini diperbarui dengan tiga AWS Application Discovery Service API —`DescribeConfigurations` ,`DescribeTags` , dan`ListConfigurations` .	10 November 2022
AWSMigrationHubStrategyCollector – Pembaruan ke kebijakan yang ada	Kebijakan ini diperbarui dengan `UpdateCollectorConfiguration` tindakan. Tindakan ini menyimpan konfigurasi kolektor Anda untuk pengambilan yang mudah.	September 07, 2022
AWSMigrationHubStrategyConsoleFullAccess— Kebijakan baru tersedia saat peluncuran	`AWSMigrationHubStrategyConsoleFullAccess` memberikan pengguna akses penuh ke layanan Rekomendasi Strategi melalui. AWS Management Console	25 Oktober 2021

Perubahan	Deskripsi	Tanggal
AWSMigrationHubStrategyCollector— Kebijakan baru tersedia saat peluncuran	`AWSMigrationHubStrategyCollector` memberikan pengguna akses ke layanan Rekomendasi Strategi dan akses baca/tulis ke bucket S3 yang terkait dengan layanan. Ini juga memberikan akses Amazon API Gateway untuk mengunggah log dan metrik ke AWS, dan AWS Secrets Manager akses untuk mengambil kredensil.	25 Oktober 2021
AWSMigrationHubStrategyServiceRolePolicy— Kebijakan baru tersedia saat peluncuran	Kebijakan peran `AWSMigrationHubStrategyServiceRolePolicy` terkait layanan menyediakan akses ke AWS Migration Hub dan. AWS Application Discovery Service Kebijakan ini juga memberikan izin untuk menyimpan laporan di Amazon Simple Storage Service (Amazon S3).	25 Oktober 2021
Rekomendasi Strategi mulai melacak perubahan	Rekomendasi Strategi mulai melacak perubahan untuk kebijakan yang AWS dikelola.	25 Oktober 2021

Contoh kebijakan berbasis identitas untuk Rekomendasi Strategi Migration Hub

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Rekomendasi Strategi. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Rekomendasi Strategi, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Rekomendasi Strategi Hub Migrasi di Referensi Otorisasi Layanan.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Rekomendasi Strategi di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS service, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Rekomendasi Strategi

Untuk mengakses konsol Rekomendasi Strategi Hub Migrasi, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Rekomendasi Strategi di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Rekomendasi Strategi, lampirkan juga Rekomendasi Strategi `ConsoleAccess` atau kebijakan `ReadOnly` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Mengakses satu bucket Amazon S3

Dalam contoh ini, Anda ingin memberikan pengguna IAM dalam Akun AWS akses Anda ke salah satu bucket Amazon S3 Anda,. `examplebucket` Anda juga ingin mengizinkan pengguna untuk menambah, memperbarui, dan menghapus objek.

Selain memberikan izin `s3:PutObject`, `s3:GetObject`, dan `s3:DeleteObject` bagi pengguna, kebijakan tersebut juga memberikan izin `s3:ListAllMyBuckets`, `s3:GetBucketLocation`, dan `s3:ListBucket`. Izin-izin tersebut adalah izin tambahan yang diperlukan oleh konsol tersebut. Selain itu, tindakan `s3:PutObjectAcl` dan `s3:GetObjectAcl` diperlukan untuk dapat menyalin, memotong, dan menempel objek di konsol. Untuk contoh panduan yang memberikan izin kepada pengguna dan mengujinya menggunakan konsol, lihat Contoh panduan: Menggunakan kebijakan pengguna untuk mengontrol akses ke bucket Anda.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
```

```
            "Sid":"ManageBucketContents",
            "Effect":"Allow",
            "Action":[
               "s3:PutObject",
               "s3:PutObjectAcl",
               "s3:GetObject",
               "s3:GetObjectAcl",
               "s3:DeleteObject"
            ],
            "Resource":"arn:aws:s3:::examplebucket/*"
         }
      ]
}
```

Pemecahan Masalah Identitas dan akses Rekomendasi Strategi Migration Hub

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Rekomendasi Strategi dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan dalam Rekomendasi Strategi
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin melihat access key saya
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses Rekomendasi Strategi
- Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Rekomendasi Strategi saya

Saya tidak berwenang untuk melakukan tindakan dalam Rekomendasi Strategi

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya fiktif *`my-example-widget`*, tetapi tidak memiliki izin fiktif `migrationhub-strategy:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 migrationhub-strategy:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya agar dia dapat mengakses *my-example-widget* menggunakan `migrationhub-strategy:`*GetWidget* tindakan.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Rekomendasi Strategi.

Beberapa AWS services memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan dalam Rekomendasi Strategi. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin melihat access key saya

Setelah membuat access key pengguna IAM, Anda dapat melihat access key ID Anda setiap saat. Namun, Anda tidak dapat melihat secret access key Anda lagi. Jika Anda kehilangan secret key, Anda harus membuat pasangan access key baru.

Access key terdiri dari dua bagian: access key ID (misalnya, `AKIAIOSFODNN7EXAMPLE`) dan secret access key (misalnya, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Seperti nama

pengguna dan kata sandi, Anda harus menggunakan access key ID dan secret access key sekaligus untuk mengautentikasi permintaan Anda. Kelola access key Anda seaman nama pengguna dan kata sandi Anda.

> **Important**
>
> Jangan memberikan access key Anda kepada pihak ke tiga, bahkan untuk membantu menemukan ID pengguna kanonis Anda. Dengan melakukan ini, Anda mungkin memberi seseorang akses permanen ke Anda Akun AWS.

Saat Anda membuat pasangan access key, Anda diminta menyimpan access key ID dan secret access key di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan secret access key Anda, Anda harus menambahkan access key baru ke pengguna IAM Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, Anda harus menghapus satu pasangan kunci sebelum membuat pasangan baru. Untuk melihat instruksi, lihat Mengelola access keys di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Rekomendasi Strategi

Untuk memungkinkan orang lain mengakses Rekomendasi Strategi, Anda harus memberikan izin kepada orang atau aplikasi yang membutuhkan akses. Jika Anda menggunakan AWS IAM Identity Center untuk mengelola orang dan aplikasi, Anda menetapkan set izin kepada pengguna atau grup untuk menentukan tingkat akses mereka. Set izin secara otomatis membuat dan menetapkan kebijakan IAM ke peran IAM yang terkait dengan orang atau aplikasi. Untuk informasi selengkapnya, lihat Set izin di Panduan AWS IAM Identity Center Pengguna.

Jika Anda tidak menggunakan IAM Identity Center, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Anda kemudian harus melampirkan kebijakan ke entitas yang memberi mereka izin yang benar dalam Rekomendasi Strategi. Setelah izin diberikan, berikan kredensialnya kepada pengguna atau pengembang aplikasi. Mereka akan menggunakan kredensyal tersebut untuk mengakses. AWSUntuk mempelajari selengkapnya tentang membuat pengguna, grup, kebijakan, dan izin IAM, lihat Identitas dan Kebijakan IAM dan izin di IAM di Panduan Pengguna IAM.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Rekomendasi Strategi saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Rekomendasi Strategi mendukung fitur-fitur ini, lihatBagaimana Rekomendasi Strategi Hub Migrasi bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk Rekomendasi Strategi

Rekomendasi Strategi Hub Migrasi menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Rekomendasi Strategi. Peran terkait layanan telah ditentukan sebelumnya oleh Rekomendasi Strategi dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Rekomendasi Strategi lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Rekomendasi Strategi mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Rekomendasi Strategi yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS Layanan yang Bekerja dengan IAM dan cari layanan yang memiliki Ya di kolom Peran Tertaut Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Rekomendasi Strategi

Rekomendasi Strategi menggunakan peran terkait layanan bernama AWSServiceRoleForMigrationHubStrategydan mengaitkannya dengan kebijakan AWSMigrationHubStrategyServiceRolePolicyIAM — Menyediakan akses ke dan. AWS Migration Hub AWS Application Discovery Service Kebijakan ini juga memberikan izin untuk menyimpan laporan di Amazon Simple Storage Service (Amazon S3).

Peran tertaut layanan AWSServiceRoleForMigrationHubStrategy memercayai layanan berikut untuk mengambil peran tersebut:

- `migrationhub-strategy.amazonaws.com`

Kebijakan izin peran memungkinkan Rekomendasi Strategi untuk menyelesaikan tindakan berikut.

AWS Application Discovery Service tindakan

```
discovery:ListConfigurations

discovery:DescribeConfigurations
```

AWS Migration Hub tindakan

```
mgh:GetHomeRegion
```

Tindakan Amazon S3

```
s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject

s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject

s3:PutObjectAcl
```

Untuk melihat izin kebijakan ini, lihat AWSMigrationHubStrategyServiceRolePolicydi Panduan Referensi Kebijakan AWS Terkelola.

Untuk melihat riwayat pembaruan kebijakan ini, lihatRekomendasi Strategi memperbarui kebijakan AWS terkelola.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi lebih lanjut, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Rekomendasi Strategi

Anda tidak perlu membuat peran terkait layanan secara manual. Jika Anda setuju untuk mengizinkan Hub Migrasi membuat peran terkait layanan (SLR) di akun Anda di akun AWS Management Console, Rekomendasi Strategi akan membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Jika Anda setuju untuk mengizinkan Hub Migrasi membuat peran terkait layanan (SLR) di akun Anda, Rekomendasi Strategi akan membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Rekomendasi Strategi

Rekomendasi Strategi tidak memungkinkan Anda untuk mengedit peran AWSServiceRoleForMigrationHubStrategyterkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan konsol Rekomendasi Strategi, CLI, atau API.

Menghapus peran terkait layanan untuk Rekomendasi Strategi

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForMigrationHubStrategyterkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Saat menghapus sumber daya Rekomendasi Strategi yang digunakan oleh AWSServiceRoleForMigrationHubStrategySLR, Anda tidak dapat menjalankan penilaian apa pun (tugas untuk menghasilkan rekomendasi). Tidak ada penilaian latar belakang yang dapat dijalankan.

Jika penilaian sedang berjalan, penghapusan SLR gagal di konsol IAM. Jika penghapusan SLR gagal, Anda dapat mencoba lagi penghapusan setelah semua tugas latar belakang selesai. Anda tidak perlu membersihkan sumber daya apa pun yang dibuat sebelum menghapus SLR.

Wilayah yang Didukung untuk Rekomendasi Strategi peran terkait layanan

Rekomendasi Strategi mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

Rekomendasi Migration Hub dan titik akhir antarmuka VPC (AWS PrivateLink)

Anda dapat membangun hubungan privat antara Rekomendasi Strategi VPC Anda dan Migration Hub dengan membuattitik akhir VPC antarmuka. Endpoint antarmuka didukung oleh AWS PrivateLink. DenganAWS PrivateLink, Anda dapat mengakses operasi API Rekomendasi Strategi tanpa gateway internet, perangkat NAT, koneksi VPN, atauAWS Direct Connectkoneksi. Instans dalam VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan operasi API Rekomendasi. Lalu lintas antara VPC Anda dan Rekomendasi Strategi tetap berada dalam jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Untuk informasi selengkapnya, lihatTitik akhir VPC antarmuka (AWS PrivateLink)diPanduan Pengguna Amazon VPC.

Pertimbangan untuk Rekomendasi Strategi endpoint VPC

Sebelum Anda menyiapkan VPC endpoint antarmuka untuk Rekomendasi Strategi, pastikan bahwa Anda meninjauProperti endpoint antarmuka dan keterbatasandanAWS PrivateLinkkuotadiPanduan Pengguna Amazon VPC.

Rekomendasi strategi mendukung panggilan ke semua tindakan API-nya dari VPC Anda. Untuk menggunakan semua Rekomendasi Strategi, Anda harus membuat endpoint VPC.

Membuat VPC endpoint antarmuka untuk Rekomendasi Strategi

Anda dapat membuat VPC endpoint untuk Rekomendasi Strategi menggunakan konsol Amazon VPC atauAWS Command Line Interface(AWS CLI). Untuk informasi lebih lanjut, lihat Membuat titik akhir antarmuka di Panduan Pengguna Amazon VPC.

Buat VPC endpoint untuk Rekomendasi Strategi menggunakan nama layanan berikut:

- `com.amazonaws.region.migrationhub-strategy`

Jika Anda menggunakan DNS privat untuk titik akhir, Anda dapat membuat permintaan API untuk Rekomendasi Strategi menggunakan nama DNS defaultnya untuk Wilayah. Misalnya, Anda dapat menggunakan nama`migrationhub-strategy.us-east-1.amazonaws.com`.

Untuk informasi lebih lanjut, lihat Mengakses layanan melalui titik akhir antarmuka di Panduan Pengguna Amazon VPC.

Membuat kebijakan VPC endpoint untuk Rekomendasi Strategi

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke Rekomendasi Strategi. Kebijakan menentukan informasi berikut ini:

- Prinsip-prinsip yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang dapat digunakan untuk mengambil tindakan.

Untuk informasi selengkapnya, lihat Mengendalikan akses ke layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan VPC endpoint untuk tindakan Rekomendasi Strategi

Berikut adalah contoh kebijakan titik akhir untuk Rekomendasi Strategi. Jika dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Rekomendasi Strategi yang terdaftar untuk semua prinsip di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "migrationhub-strategy:ListContacts",
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

Validasi kepatuhan untuk Rekomendasi Strategi Migration Hub

Untuk mempelajari apakah an AWS service berada dalam lingkup program kepatuhan tertentu, lihat AWS services di Lingkup oleh Program Kepatuhan AWS services dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan AWS services ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi AWS services syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan AWS services dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.

- AWS Security Hub— Ini AWS service memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini AWS service mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni AWS service membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Bekerja dengan layanan yang lain

Bagian ini menjelaskan lainnyaAWSlayanan yang berinteraksi dengan Migration Hub Rekomendasi Strategi.

Topik

Mencatat log panggilan API Rekomendasi Strategi denganAWS CloudTrail

Migration Hub Rekomendasi Strategi terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWSlayanan di Rekomendasi Strategi. CloudTrail merekam panggilan API untuk Rekomendasi Strategi sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsol Rekomendasi Strategi dan panggilan kode ke operasi API Rekomendasi Strategi.

Jika membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan peristiwa CloudTrail ke bucket Amazon S3, termasuk peristiwa untuk Rekomendasi Strategi. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam konsol CloudTrail di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Rekomendasi Strategi, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk mempelajari selengkapnya tentang CloudTrail, lihat Panduan Pengguna AWS CloudTrail.

Informasi rekomendasi strategi di CloudTrail

CloudTrail diaktifkan di Akun AWS Anda saat Anda membuat akun. Saat aktivitas terjadi di Rekomendasi Strategi, aktivitas itu dicatat di CloudTrail bersama rekomendasi lainnyaAWSperistiwa layanan diRiwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi lebih lanjut, lihat Melihat peristiwa dengan riwayat CloudTrail Event.

Untuk catatan berkelanjutan tentang peristiwa diAkun AWS, termasuk acara untuk Rekomendasi Strategi, buat jejak. Jejak memungkinkan CloudTrail mengirim file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS.

Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi layanan AWS lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di log CloudTrail. Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk membuat jejak
- Layanan dan Integrasi CloudTrail yang Didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima Berkas Log CloudTrail dari Beberapa Wilayah dan Menerima Berkas Log CloudTrail dari Beberapa Akun

Rekomendasi strategi mendukung pencatatan tindakan berikut sebagai peristiwa di berkas log CloudTrail:

- getApplicationComponentStrategies
- GetApplicationComponentDetails
- GetAssesment
- getImportFileTask
- GetPortofolioPreferensi
- getPortofolioSummary
- GetServerDetails
- GetServerStrategies
- ListApplicationComponents
- ListCollectors
- ListimportFileTask
- ListServers
- PutportfolioPreferensi
- startAssessment
- StartImportFileTask
- stopAssessment
- UpdateApplicationComponetConfig
- UpdateServerConfig

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Jika permintaan tersebut dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM)
- Jika permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi selengkapnya, lihat elemen userIdentity CloudTrail.

Memahami entri berkas log

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. File log CloudTrail berisi satu atau beberapa entri log. Peristuwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. File log CloudTrail bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri log CloudTrail yang menunjukkan entri log CloudTrail yang menunjukkanGetServerDetailstindakan.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2021-09-20T01:07:16Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-09-20T01:07:43Z",
    "eventSource": "migrationhub-strategy.amazonaws.com",
    "eventName": "GetServerDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "",
    "requestParameters": {
        "serverId": "ads-server-006"
    },
    "responseElements": null,
    "requestID": "07D681279BD94AED",
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Kuota untuk Rekomendasi Strategi Migration Hub

Akun AWS Anda memiliki kuota default, yang sebelumnya disebut sebagai batas, untuk setiap layanan AWS. Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat daftar kuota Rekomendasi Strategi Migration Hub, lihatKuota layanan rekomendasi.

Anda juga dapat melihat kuota untuk Rekomendasi Strategi, dengan membukaService Quotas Console. Di panel navigasi, pilihAWSjasadan pilihRekomendasi Strategi Migration Hub.

Untuk meminta kenaikan kuota, lihat Meminta kenaikan Kuota dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan kuota layananFormulir kenaikan batas.

Catatan perilisan

Topik

17 November 2023

Fitur baru

- Kolektor v1.1.47
- Support untuk aplikasi.NET 8.

12 Oktober 2023

Fitur baru

- Kolektor v1.1.45
- Support untuk sumber Multi-data.

17 April 2023

Fitur baru

- Kolektor v1.1.22
- Tingkatkan penyempurnaan skrip. Ini membutuhkan versi terbaru dari Kolektor.

Maret 17, 2023

Fitur baru

Menambahkan analisis biner, yang menyediakan deteksi anti-pola dan ketidakcocokan tanpa kode sumber.

November 07, 2022

Fitur baru

- Pemfilteran aplikasi untuk aplikasi
- Pemfilteran server berdasarkan tag AWS Application Discovery Service

September 27, 2022

Fitur baru

- Kolektor v1.1.12
  - SCT versi 667
  - Empanalyzer 2.2.0.368
- Menambahkan `diag check` perintah untuk wawasan server.
- Menambahkan dukungan untuk rekomendasi Potensi.
- Antarmuka pengguna yang disempurnakan untuk memeriksa konfigurasi dan status penilaian.

Perbaikan bug

- Porting asisten penerjemah dan perbaikan lainnya.

30 Juni 2022

Fitur baru

- Kolektor v1.1.11
  - Menambahkan dukungan API VMware.
  - A2C meminta perubahan untuk menambahkan header pengguna saat mengunduh file biner.
  - Menambahkan home path Linux, shell default, dan terminasi jarak jauh dari semua shell.
- A2C v1.17 biner publik
  - Menambahkan dukungan untuk Azure DevOps sebagai target penerapan pipeline.

April 18, 2022

Fitur baru

- Kolektor v1.1.7
- Menambahkan kemampuan untuk mengunduh biner A2C secara dinamis dari URL publik.

Perbaikan bug

- A2C v1.1.5

25 Februari 2022

Perbaikan bug

- SCT v5.6.9
- A2C v1.1.2
- Kolektor v1.1.4

Februari 10, 2022

Perbaikan bug

- SCT v5.6.8

- A2C v1.1.1
  - Menambahkan cek untuk tar perintah di Linux.
  - Memperbaiki masalah memeriksa gambar aplikasi di Amazon ECR.
  - Memperbaiki masalah yang membutuhkan penghapusan kontainer untuk pra-validasi.
- Kolektor v1.1.3
  - Memperbaiki kesalahan 4xx untuk mesin 32-bit jarak jauh.
  - Memperbarui kode kesalahan A2C.
  - Memvalidasi alamat IP C# untuk analisis kode sumber mesin jarak jauh.

28 Januari 2022

Fitur baru

- Kolektor v1.1.2
- Menambahkan dukungan DevOps repositori Azure Git untuk analisis kode sumber.

Januari 14, 2022

Fitur baru

- Kolektor v1.1.1
- Menambahkan rekomendasi Babelfish untuk database SQL.

Desember 21, 2021

Masalah teratasi

- Kolektor v1.1.0
- Analisis basis data telah dipulihkan.

Desember 15, 2021

Masalah yang diketahui

- Kolektor v1.0.4
- Analisis basis data saat ini tidak didukung (CVE-2021-44228).

Oktober 25, 2021

Fitur baru

- Kolektor v1.0.0
- Rilis awal Panduan Pengguna Rekomendasi Strategi Hub Migrasi.

Riwayat dokumen dan versi

Tabel berikut menjelaskan rilis dokumentasi untuk Rekomendasi Strategi. Untuk informasi selengkapnya, lihat Catatan perilisan.

Ubah	Deskripsi	Tanggal
AWS pembaruan kebijakan terkelola - perbarui ke AWSMigrationHubStrategyCollector	Memperbarui AWSMigrationHubStrategyCollectorkebijakan untuk menyertakan barus3,`application-transformation` , dan `migrationhub-strategy` tindakan.	April 1, 2024
AWS pembaruan kebijakan terkelola - perbarui ke AWSMigrationHubStrategyCollector	Memperbarui AWSMigrationHubStrategyCollectorkebijakan untuk menyertakan `application-transformation` tindakan baru. Pembaruan ini juga menambahkan kondisi untuk membatasi berbagai tindakan di mana `aws:ResourceAccount` harus sama dengan. `aws:PrincipalAccount`	Februari 5, 2024
Fitur baru	Rekomendasi Strategi klien pengumpul data aplikasi v1.1.47 tersedia dengan dukungan untuk aplikasi.NET 8.	17 November 2023
Fitur baru	Rekomendasi Strategi klien pengumpul data aplikasi	12 Oktober 2023

	v1.1.45 tersedia dengan dukungan untuk Beberapa sumber data.	
AWS pembaruan kebijakan terkelola - perbarui ke AWSMigrationHubStrategyCollector	Memperbarui AWSMigrationHubStrategyCollectorkebijakan untuk menyertakan API Amazon S3 baru.	15 September 2023
AWS pembaruan kebijakan terkelola - perbarui ke AWSMigrationHubStrategyCollector	Memperbarui AWSMigrationHubStrategyCollectorkebijakan untuk menyertakan penganalisis baru untuk kode sumber.	8 Maret 2023
Pembaruan praktik terbaik IAM	Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	Februari 25, 2023
AWS pembaruan kebijakan terkelola - pembaruan ke kebijakan yang ada	Rekomendasi Strategi Migration Hub menambahkan tiga AWS Application Discovery Service API yang ditambahkan ke kebijakan yang ada.	10 November 2022
Pembaruan keamanan	Buat koneksi pribadi dengan antarmuka VPC endpoint.	07 Maret, 2022
Fitur baru	Menambahkan dukungan DevOps repositori Azure Git untuk analisis kode sumber.	28 Januari 2022
Fitur baru	Menambahkan rekomendasi Babelfish untuk database SQL.	Januari 14, 2022

Rilis awal	Rilis awal Panduan Pengguna Rekomendasi Strategi Hub Migrasi.	25 Oktober 2021

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