Panduan Pengguna

AWS Application Discovery Service

AWS Application Discovery Service: Panduan Pengguna

Table of Contents

Apa itu AWS Application Discovery Service? 1
VMware Penemuan 2
Penemuan basis data 3
Bandingkan Kolektor Tanpa Agen dan Agen Penemuan 3
Asumsi 6
AWS Application Discovery Service perubahan ketersediaan 8
Detail ketersediaan layanan 8
AWS Transform transisi 8
Pertanyaan umum 9
Menyiapkan 11
Mendaftar Amazon Web Services 11
Buat pengguna IAM 11
Membuat Pengguna Administratif IAM 12
Membuat Pengguna Non-Administratif IAM 12
Masuk ke Migration Hub dan pilih Wilayah beranda 13
Discovery Agent 14
Cara kerjanya 14
Data yang dikumpulkan 15
Prasyarat 18
Instalasi Discovery Agent 19
Instal di Linux 19
Instal di Microsoft Windows 23
Mengelola proses Discovery Agent 27
Kelola proses di Linux 28
Kelola proses di Microsoft Windows 29
Menghapus Instalasi Discovery Agent 30
Copot instalasi di Linux 30
Copot pemasangan di Microsoft Windows 30
Memulai dan menghentikan pengumpulan data 31
Pemecahan Masalah Agen Penemuan 32
Memecahkan Masalah Agen Penemuan di Linux 32
Memecahkan Masalah Agen Penemuan di Microsoft Windows 33
Kolektor Tanpa Agen 35
Prasyarat 35

Konfigurasikan perimeter data 36
Konfigurasikan firewall 37
Menyebarkan kolektor 38
Mmebuat pengguna IAM 38
Unduh kolektor 41
Menyebarkan kolektor 42
Mengakses konsol kolektor 43
Mengkonfigurasi kolektor 44
(Opsional) Konfigurasikan alamat IP statis untuk VM kolektor 45
(Opsional) Setel ulang VM kolektor kembali menggunakan DHCP 51
(Opsional) Konfigurasikan Kerberos 53
Menggunakan modul Pengumpulan Data Jaringan 54
Menyiapkan modul Pengumpulan Data Jaringan 55
Upaya pengumpulan data jaringan 57
Status server dalam modul Pengumpulan Data Jaringan 57
Menggunakan modul pengumpulan VMware data 58
Menyiapkan pengumpulan data vCenter 58
Melihat detail pengumpulan VMware data 59
Mengontrol ruang lingkup pengumpulan data 60
Data yang dikumpulkan oleh VMware modul 62
Menggunakan modul pengumpulan data database dan analitik 66
Server yang didukung 67
Membuat pengumpul AWS DMS data 68
Mengkonfigurasi penerusan data 69
Menambahkan server LDAP dan OS 70
Menemukan database Anda 72
Data yang dikumpulkan oleh database dan modul analitik 77
Melihat data yang dikumpulkan 79
Mengakses Kolektor Tanpa Agen 80
Dasbor kolektor 80
Mengedit pengaturan kolektor 82
Mengedit kredensi vCenter 83
Memperbarui Kolektor Tanpa Agen 84
Pemecahan masalah 85
Memperbaiki `Unable to retrieve manifest or certificate file error` 86

Mengatasi masalah sertifikasi yang ditandatangani sendiri saat mengonfigurasi sertifikat WinRM 86
Memperbaiki Agentless Collector tidak dapat mencapai AWS selama pengaturan 87
Memperbaiki masalah sertifikasi yang ditandatangani sendiri saat menghubungkan ke host proxy 89
Menemukan kolektor yang tidak sehat 90
Memperbaiki masalah alamat IP 91
Memperbaiki masalah kredensil vCenter 91
Memperbaiki masalah penerusan data 92
Memperbaiki masalah koneksi 92
Dukungan host ESX mandiri 94
Menghubungi AWS Support 94
Mengimpor data ke Migration Hub 96
Format impor yang didukung 96
RVTools 97
Templat impor Hub Migrasi 97
Menyiapkan izin impor 102
Mengunggah file impor Anda ke Amazon S3 106
Mengimpor data 107
Melacak permintaan impor Hub Migrasi 109
Lihat dan jelajahi data 111
Lihat data yang dikumpulkan 111
Logika pencocokan 112
Menjelajahi data di Athena 113
Mengaktifkan eksplorasi data 113
Menjelajahi data 115
Memvisualisasikan data 116
Menggunakan kueri yang telah ditentukan 117
Menemukan data dengan konsol Migration Hub 125
Melihat data di dasbor 125
Memulai dan menghentikan pengumpul data 126
Menyortir pengumpul data 126
Melihat server 130
Menyortir server 131
Menandai server 131
Mengekspor data server 132

Pengelompokan server 134
Menggunakan API untuk menanyakan item yang ditemukan 136
Menggunakan `DescribeConfigurations` tindakan 136
Menggunakan `ListConfigurations` tindakan 140
Konsistensi akhirnya 155
AWS PrivateLink 157
Pertimbangan-pertimbangan 157
Membuat sebuah titik akhir antarmuka 157
Membuat kebijakan titik akhir 158
Menggunakan titik akhir VPC untuk Agentless Collector dan Application Discovery Agent AWS 159
Keamanan 161
Identity and Access Management 162
Audiens 162
Mengautentikasi dengan identitas 163
Mengelola akses menggunakan kebijakan 164
Bagaimana AWS Application Discovery Service bekerja dengan IAM 166
AWS kebijakan terkelola 168
Contoh kebijakan berbasis identitas 174
Memahami dan menggunakan peran terkait layanan 182
Menyelesaikan masalah IAM 189
Pencatatan panggilan API dengan CloudTrail 190
Informasi Application Discovery Service di CloudTrail 191
Memahami entri berkas log Application Discovery Service 192
Format ARN 194
Kuota 195
Pemecahan Masalah 196
Hentikan pengumpulan data dengan eksplorasi data 196
Hapus data yang dikumpulkan oleh eksplorasi data 197
Perbaiki masalah umum dengan eksplorasi data di Amazon Athena 198
Eksplorasi data di Amazon Athena gagal dimulai karena peran terkait layanan dan AWS sumber daya yang diperlukan tidak dapat dibuat 199
Data Agen Baru tidak muncul di Amazon Athena 199
Anda tidak memiliki izin yang cukup untuk mengakses Amazon S3, Amazon Data Firehose, atau AWS Glue 201
Memecahkan masalah catatan impor yang gagal 201

Riwayat Dokumen 204
AWS Glosarium 209
..... ccx

Apa itu AWS Application Discovery Service?

AWS Application Discovery Service membantu Anda merencanakan migrasi ke AWS cloud dengan mengumpulkan data penggunaan dan konfigurasi tentang server dan database lokal Anda. Application Discovery Service terintegrasi dengan AWS Migration Hub dan AWS Database Migration Service Fleet Advisor. Migration Hub menyederhanakan pelacakan migrasi Anda karena menggabungkan informasi status migrasi Anda ke dalam satu konsol. Anda dapat melihat server yang ditemukan, mengelompokkannya ke dalam aplikasi, lalu melacak status migrasi setiap aplikasi dari konsol Hub Migrasi di Wilayah asal Anda. Anda dapat menggunakan DMS Fleet Advisor untuk menilai opsi migrasi untuk beban kerja database.

Semua data yang ditemukan disimpan di Wilayah AWS Migration Hub asal Anda. Oleh karena itu, Anda harus menyetel Wilayah rumah Anda di konsol Migration Hub atau dengan perintah CLI sebelum melakukan aktivitas penemuan dan migrasi apa pun. Data Anda dapat diekspor untuk analisis di Microsoft Excel atau alat AWS analisis seperti Amazon Athena dan Amazon Quick.

Menggunakan Application Discovery Service APIs, Anda dapat mengekspor kinerja sistem dan data pemanfaatan untuk server yang Anda temukan. Masukkan data ini ke dalam model biaya Anda untuk menghitung biaya menjalankan server tersebut. AWS Selain itu, Anda dapat mengekspor data tentang koneksi jaringan antarserver. Informasi ini membantu Anda menentukan dependensi jaringan antarserver dan mengelompokkannya ke dalam aplikasi untuk perencanaan migrasi.

> **Note**
>
> Wilayah asal Anda harus diatur AWS Migration Hub sebelum Anda memulai proses penemuan, karena data Anda akan disimpan di Wilayah asal Anda. Untuk informasi lebih lanjut tentang bekerja dengan Wilayah asal, lihat Wilayah Asal.

Application Discovery Service menawarkan tiga cara untuk melakukan penemuan dan pengumpulan data tentang server lokal Anda:

- Penemuan tanpa agen dapat dilakukan dengan menggunakan Application Discovery Service Agentless Collector (Agentless Collector) (file OVA) melalui vCenter Anda. VMware Setelah Agentless Collector dikonfigurasi, ia mengidentifikasi mesin virtual (VMs) dan host yang terkait dengan vCenter. Agentless Collector mengumpulkan data konfigurasi statis berikut: Nama host server, alamat IP, alamat MAC, alokasi sumber daya disk, versi mesin database, dan skema

database. Selain itu, ia mengumpulkan data pemanfaatan untuk setiap VM dan database yang menyediakan pemanfaatan rata-rata dan puncak untuk metrik seperti CPU, RAM, dan Disk I/O.

- Penemuan berbasis agen dapat dilakukan dengan menggunakan AWS Application Discovery Agent (Discovery Agent) pada setiap server Anda VMs dan fisik. Penginstal agen tersedia untuk sistem operasi Windows dan Linux. Alat ini mengumpulkan data konfigurasi statis, informasi detail performa sistem deret waktu, koneksi jaringan inbound dan outbound, serta proses yang sedang berjalan.
- Impor berbasis file memungkinkan Anda mengimpor detail lingkungan lokal langsung ke Migration Hub tanpa menggunakan Agentless Collector atau Discovery Agent, sehingga Anda dapat melakukan penilaian dan perencanaan migrasi langsung dari data yang diimpor. Data yang dicerna tergantung pada data yang diberikan.

Application Discovery Service terintegrasi dengan solusi penemuan aplikasi dari AWS mitra Partner Network (APN). Solusi pihak ketiga ini dapat membantu Anda mengimpor detail tentang lingkungan lokal langsung ke Migration Hub, tanpa menggunakan kolektor atau agen penemuan tanpa agen apa pun. Alat penemuan aplikasi pihak ketiga dapat meminta AWS Application Discovery Service, dan mereka dapat menulis ke database Application Discovery Service menggunakan API publik. Dengan cara ini, Anda dapat mengimpor data ke Migration Hub dan melihatnya, sehingga Anda dapat mengaitkan aplikasi dengan server dan melacak migrasi.

VMware Penemuan

Jika Anda memiliki mesin virtual (VMs) yang berjalan di lingkungan VMware vCenter, Anda dapat menggunakan Agentless Collector untuk mengumpulkan informasi sistem tanpa harus menginstal agen pada setiap VM. Sebagai gantinya, Anda memuat alat lokal ini ke dalam vCenter dan memungkinkannya menemukan semua hostnya dan. VMs

Agentless Collector menangkap informasi kinerja sistem dan pemanfaatan sumber daya untuk setiap VM yang berjalan di vCenter, terlepas dari sistem operasi apa yang digunakan. Namun, tidak dapat “melihat ke dalam” masing-masing VMs, dan dengan demikian, tidak dapat mengetahui proses apa yang berjalan pada setiap VM atau koneksi jaringan apa yang ada. Oleh karena itu, jika Anda memerlukan tingkat detail ini dan ingin melihat lebih dekat beberapa yang ada VMs untuk membantu merencanakan migrasi Anda, Anda dapat menginstal Agen Penemuan sesuai kebutuhan.

Selain itu, untuk VMs di-host VMware, Anda dapat menggunakan Agentless Collector dan Discovery Agent untuk melakukan penemuan secara bersamaan. Untuk detail mengenai jenis data yang tepat

yang akan dikumpulkan oleh setiap alat penemuan, lihatMenggunakan modul pengumpulan VMware data vCenter Agentless Collector.

Penemuan basis data

Jika Anda memiliki server database dan analitik di lingkungan lokal, Anda dapat menggunakan Agentless Collector untuk menemukan dan menginventarisasi server ini. Anda kemudian dapat mengumpulkan metrik kinerja untuk setiap server database tanpa perlu menginstal Agentless Collector di setiap komputer di lingkungan Anda.

Database Agentless Collector dan modul pengumpulan data analitik menangkap metadata dan metrik kinerja yang memberikan wawasan tentang infrastruktur data Anda. Modul pengumpulan data database dan analitik menggunakan LDAP di Microsoft Active Directory untuk mengumpulkan informasi tentang OS, database, dan server analitik di jaringan Anda. Kemudian, modul pengumpulan data secara berkala menjalankan kueri untuk mengumpulkan metrik pemanfaatan aktual CPU, memori, dan kapasitas disk untuk database dan server analitik. Untuk detail mengenai metrik yang dikumpulkan, lihatData yang dikumpulkan oleh database dan modul analitik.

Setelah Agentless Collector menyelesaikan pengumpulan data dari lingkungan Anda, Anda dapat menggunakan AWS DMS konsol untuk analisis lebih lanjut dan untuk merencanakan migrasi Anda. Misalnya, untuk memilih target migrasi yang optimal AWS Cloud, Anda dapat membuat rekomendasi target untuk basis data sumber Anda. Untuk informasi selengkapnya, lihat Menggunakan modul pengumpulan data database dan analitik.

Bandingkan Kolektor Tanpa Agen dan Agen Penemuan

Tabel berikut memberikan perbandingan cepat dari metode pengumpulan data yang didukung Application Discovery Service.

	Kolektor Tanpa Agen	Discovery Agent	Templat Hub Migrasi	RVTools ekspor
Supported server types				
VMware mesin virtual	Ya	Ya	Ya	Ya
Server fisik	Tidak	Ya	Ya	Ya

	Kolektor Tanpa Agen	Discovery Agent	Templat Hub Migrasi	RVTools ekspor
Deployment				
Per server	Tidak	Ya	N/A	Tidak
Per vCenter	Ya	Tidak	N/A	Ya
Per pusat data pada jaringan yang sama	Tidak	Tidak	N/A	Tidak
Collected data				
Data profil server (konfigurasi statis)	Ya	Ya	Ya	Ya
Metrik pemanfaatan server dari Hypervisor (CPU, RAM, dll.)	Ya	Ya	Ya	Tidak
Metrik pemanfaatan server dari server (CPU, RAM, dll.)	Ya	Ya	Ya	Tidak
Koneksi jaringan server (hanya TCP)	Ya	Ya	Tidak	Tidak
Proses berjalan	Tidak	Ya	Tidak	Tidak
Interval pengumpulan	-60 menit	-15 detik	Cuplikan tunggal	Cuplikan tunggal
Server data use cases				

	Kolektor Tanpa Agen	Discovery Agent	Templat Hub Migrasi	RVTools ekspor
Melihat data server di Migration Hub	Ya	Ya	Profil saja	Tidak
Hasilkan rekomendasi Amazon EC2 berdasarkan profil server	Ya	Ya	Ya	Ya
Hasilkan rekomendasi Amazon EC2 berdasarkan data pemanfaatan	Ya	Ya	Ya	Tidak
Ekspor data snapshot pemanfaatan terbaru	Ya	Ya	Ya	Tidak
Ekspor data pemanfaatan deret waktu	Tidak	Ya	Tidak	Tidak
Network data use cases				
Visualisasi di Migration Hub	Ya	Ya	Tidak	Tidak
Ekspor ke Amazon Athena untuk eksplorasi lebih lanjut	Tidak	Ya	Tidak	Tidak

	Kolektor Tanpa Agen	Discovery Agent	Templat Hub Migrasi	RVTools ekspor
Ekspor ke file CSV	Tidak	Ya	Tidak	Tidak
Database use cases				
Data profil server basis data (konfigurasi statis)	Ya	Tidak	Tidak	Tidak
Mesin basis data yang didukung	Oracle, SQL Server, MySQL, PostgreSQL	Tidak ada	Tidak ada	Tidak ada
Kompleksitas skema database dan duplikat	Ya	Tidak	Tidak	Tidak
Objek skema database	Ya	Tidak	Tidak	Tidak
Platform support				
Sistem operasi yang didukung	OS apa pun yang berjalan di VMware tengah v5.5 atau versi yang lebih baru	Server Linux atau Windows apa pun	Server Linux atau Windows apa pun	Server Linux, server Windows, atau VMware v5.5 atau versi yang lebih baru

Asumsi

Untuk menggunakan Application Discovery Service, hal-hal berikut ini diasumsikan:

- Anda telah mendaftar untuk AWS. Untuk informasi selengkapnya, lihat Menyiapkan Application Discovery Service.

- Anda telah memilih Wilayah beranda Hub Migrasi. Untuk informasi lebih lanjut, lihat dokumentasi mengenai Wilayah asal.

Berikut ini yang akan berlaku:

- Wilayah asal Migration Hub adalah satu-satunya Wilayah tempat Application Discovery Service menyimpan data penemuan dan perencanaan Anda.
- Agen penemuan, konektor, dan impor hanya dapat digunakan di Wilayah asal Migration Hub pilihan Anda.
- Untuk daftar AWS Wilayah tempat Anda dapat menggunakan Application Discovery Service, lihat Referensi Umum Amazon Web Services.

AWS Application Discovery Service perubahan ketersediaan

Setelah mempertimbangkan dengan cermat, kami memutuskan AWS Application Discovery Service untuk menutup pelanggan baru mulai 7 November 2025. Jika Anda ingin menggunakan layanan ini, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa.

Topik ini memberikan informasi tentang perubahan ketersediaan dan panduan untuk transisi ke. AWS Transform

Detail ketersediaan layanan

Application Discovery Service akan berhenti menerima pelanggan baru mulai 7 November 2025. AWS Transform adalah layanan AI agen generasi berikutnya yang menyediakan kemampuan serupa dan kemampuan penemuan dan penilaian VM yang disempurnakan. Pelanggan Application Discovery Service yang ada dapat terus menggunakan layanan untuk menyelesaikan proyek penemuan mereka yang sedang berlangsung, yang biasanya memiliki siklus hidup 4 bulan. Fungsionalitas inti layanan untuk menemukan dan mengumpulkan data tentang server dan aplikasi lokal sekarang tersedia AWS Transform dengan fitur yang ditingkatkan, tidak memerlukan upaya pelanggan untuk transisi.

Hingga 7 November 2025, kami akan terus menjaga keamanan dan keandalan Application Discovery Service. Meskipun kami tidak akan menambahkan fitur baru ke layanan, kami tetap berkomitmen untuk menyediakan pembaruan keamanan dan menjaga ketersediaan layanan untuk memastikan proyek migrasi Anda yang sedang berlangsung terus berjalan dengan lancar. Fokus kami adalah memastikan lingkungan yang stabil bagi pelanggan yang sudah ada untuk menyelesaikan inisiatif migrasi dalam penerbangan mereka sambil mempersiapkan peningkatan kemampuan yang tersedia di. AWS Transform

AWS Transform transisi

AWS Transform adalah solusi kami yang direkomendasikan yang menyatukan semua kemampuan Application Discovery Service sambil memperkenalkan fitur-fitur baru yang canggih. Ini memberikan kemampuan penemuan dan penilaian yang komprehensif melalui kolektor berbasis agen dan tanpa agen, dengan analisis lingkungan yang ditingkatkan. VMware Layanan ini memungkinkan pemetaan ketergantungan aplikasi otomatis dan perencanaan gelombang, sambil menawarkan

logika penemuan yang lebih baik dengan analisis bagaimana-jika dan perkiraan biaya. Dengan fitur-fitur canggih termasuk penyimpanan terintegrasi dan penemuan basis data, integrasi alat 3P terkonsolidasi, dan analisis konfigurasi VM yang komprehensif, AWS Transform dirancang untuk membuat penilaian migrasi dan proses perencanaan pelanggan lebih efisien dan sukses.

Transisi ke sangat AWS Transform mudah, tanpa diperlukan migrasi data. Proyek penemuan yang ada di Application Discovery Service akan terus berfungsi secara normal hingga selesai. Ketika pelanggan siap untuk memulai proyek penemuan baru, mereka dapat mulai menggunakan AWS Transform secara langsung - semua kemampuan penemuan dan penilaian dari Application Discovery Service tersedia di sana dengan fitur yang disempurnakan. Untuk mulai menggunakan AWS Transform silakan lihat Panduan Memulai. AWS Tim Support tersedia melalui konsol AWS Support untuk membantu AWS Transform akses atau pertanyaan tentang proyek penemuan yang sedang berlangsung.

Pertanyaan umum

Apa artinya ini bagi layanan (apakah Anda akan mematikan layanan)?

Application Discovery Service akan berhenti menerima pelanggan baru mulai 7 November 2025. Layanan ini akan terus beroperasi bagi pelanggan yang sudah ada untuk menyelesaikan proyek migrasi mereka yang sedang berlangsung.

Bagaimana pelanggan yang ada akan terpengaruh?

Pelanggan yang sudah ada tidak akan mengalami gangguan apa pun pada proyek migrasi mereka saat ini. Mereka dapat terus menggunakan Application Discovery Service seperti biasa sampai proyek mereka selesai. Semua proyek yang sedang berlangsung akan tetap dapat diakses, dan pembaruan keamanan akan terus diterapkan untuk menjaga keandalan layanan.

Pada 7 November 2025, pelanggan mengalami masalah, bagaimana mereka bisa meningkat?

Pelanggan yang mengalami masalah dapat menghubungi AWS Support melalui konsol AWS Support mereka. Tim AWS Support tersedia untuk membantu dengan pertanyaan atau masalah terkait layanan.

Alternatif apa yang dapat dijelajahi pelanggan?

AWS Transform adalah layanan alternatif yang direkomendasikan. Diluncurkan pada tahun 2025, AWS Transform mencakup kemampuan Application Discovery Service yang serupa. Menawarkan

fitur yang disempurnakan dengan analisis VMware lingkungan yang ditingkatkan dan pemetaan ketergantungan otomatis. Menyediakan penyimpanan terintegrasi dan kemampuan penemuan database dan alat penilaian yang komprehensif. Tidak diperlukan perkakas khusus saat beralih ke. AWS Transform

Bagaimana pelanggan dapat bermigrasi dari Application Discovery Service?

Tidak diperlukan proses migrasi formal. Proyek yang ada dapat dilanjutkan di Application Discovery Service hingga selesai. Untuk proyek baru, pelanggan dapat memulai secara langsung AWS Transform, yang menyediakan semua kemampuan Application Discovery Service yang sudah dikenal dengan fitur yang disempurnakan. Tidak diperlukan migrasi data, dan AWS Support tersedia untuk membantu transisi.

Jika Anda memiliki pertanyaan tambahan, silakan hubungi kami melalui AWS Support atau baca kami FAQs.

Menyiapkan Application Discovery Service

Sebelum Anda menggunakan AWS Application Discovery Service untuk pertama kalinya, selesaikan tugas-tugas berikut:

Mendaftar Amazon Web Services

Buat pengguna IAM

Masuk ke konsol Migration Hub dan pilih Wilayah beranda

Mendaftar Amazon Web Services

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/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS 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.

Buat pengguna IAM

Saat membuat AWS akun, Anda mendapatkan satu identitas masuk yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna root AWS akun. Masuk ke Konsol Manajemen AWS menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun memberi Anda akses lengkap ke semua sumber AWS daya di akun Anda.

Kami sangat menyarankan agar Anda tidak menggunakan akun pengguna root untuk tugas sehari-hari, bahkan tugas administratif. Sebagai gantinya, ikuti praktik terbaik keamanan Buat Pengguna IAM Individu dan buat pengguna administrator AWS Identity and Access Management (IAM).

Kemudian, kunci kredensial pengguna akar dengan aman dan gunakan kredensial itu untuk melakukan beberapa tugas manajemen akun dan layanan saja.

Selain membuat pengguna administratif, Anda juga perlu membuat pengguna IAM non-administratif. Topik berikut menjelaskan cara membuat kedua jenis pengguna IAM.

Topik

- Membuat Pengguna Administratif IAM
- Membuat Pengguna Non-Administratif IAM

Membuat Pengguna Administratif IAM

Secara default, akun administrator mewarisi semua kebijakan yang diperlukan untuk mengakses Application Discovery Service.

Untuk membuat pengguna administrator

- Buat pengguna administrator di AWS akun Anda. Untuk melihat instruksi, buka Membuat Grup Pengguna dan Administrator IAM Pertama Anda di Panduan Pengguna IAM.

Membuat Pengguna Non-Administratif IAM

Saat membuat pengguna IAM non-administratif, ikuti praktik terbaik keamanan dengan Berikan Hak Istimewa Minimum, untuk memberikan izin minimum kepada pengguna.

Gunakan kebijakan terkelola IAM untuk menentukan tingkat akses ke Application Discovery Service oleh pengguna IAM non-administratif. Untuk informasi tentang kebijakan terkelola Application Discovery Service, lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.

Untuk membuat pengguna IAM non-administrator

1. Masuk Konsol Manajemen AWS, navigasikan ke konsol IAM.
2. Buat pengguna IAM non-administrator dengan mengikuti petunjuk untuk membuat pengguna dengan konsol seperti yang dijelaskan dalam Membuat pengguna IAM di AWS akun Anda di Panduan Pengguna IAM.

   Sambil mengikuti petunjuk dalam Panduan Pengguna IAM:

- Saat berada di langkah tentang halaman Setel izin, pilih opsi untuk Melampirkan kebijakan yang ada ke pengguna secara langsung. Kemudian pilih kebijakan IAM terkelola untuk Application Discovery Service dari daftar kebijakan. Untuk informasi tentang kebijakan terkelola Application Discovery Service, lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.
- Ketika pada langkah tentang melihat kunci akses pengguna (kunci akses IDs dan kunci akses rahasia), ikuti panduan di Catatan penting tentang menyimpan ID kunci akses baru pengguna dan kunci akses rahasia di tempat yang aman dan terlindungi.

3. Setelah Anda membuat pengguna, berikan mereka akses terprogram seperti yang dijelaskan dalam Support akses pengguna terprogram.

Masuk ke konsol Migration Hub dan pilih Wilayah beranda

Anda harus memilih Wilayah AWS Migration Hub rumah di AWS akun yang Anda gunakan untuk AWS Application Discovery Service.

Untuk memilih Wilayah rumah

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub, pilih Pengaturan dan pilih Wilayah beranda.

   Data Hub Migrasi Anda disimpan di Wilayah asal Anda untuk tujuan penemuan, perencanaan, dan pelacakan migrasi. Untuk informasi selengkapnya, lihat Wilayah Beranda Hub Migrasi.

AWS Agen Penemuan Aplikasi

AWS Application Discovery Agent (Discovery Agent) adalah perangkat lunak yang Anda instal di server lokal dan VM yang ditargetkan untuk penemuan dan migrasi. Agen mengambil konfigurasi sistem, performa sistem, proses yang berjalan, dan detail koneksi jaringan antara sistem. Agen mendukung sebagian besar sistem operasi Linux dan Windows, dan Anda dapat men-deploy agen di server on-premise fisik, instans Amazon EC2, dan mesin virtual.

> **Note**
>
> Sebelum menerapkan Agen Penemuan, Anda harus memilih Region beranda Migration Hub. Anda harus mendaftarkan agen Anda di wilayah asal Anda.

Discovery Agent berjalan di lingkungan lokal Anda dan memerlukan hak akses root. Ketika Anda memulai Discovery Agent, Discovery Agent terhubung dengan wilayah asal Anda dengan aman dan mendaftar ke Application Discovery Service.

- Misalnya, jika `eu-central-1` adalah Wilayah asal Anda, itu mendaftar `arsenal-discovery.`*`eu-central-1`*`.amazonaws.com` dengan Application Discovery Service.
- Atau ganti Wilayah asal Anda sesuai kebutuhan untuk semua Wilayah lain kecuali us-west-2.
- Jika `us-west-2` adalah Wilayah asal Anda, itu mendaftar `arsenal.us-west-2.amazonaws.com` dengan Application Discovery Service.

Cara kerjanya

Setelah pendaftaran, agen mulai mengumpulkan data untuk host atau VM di mana ia berada. Agen mengirim ping ke Application Discovery Service pada interval 15 menit untuk informasi konfigurasi.

Data yang dikumpulkan mencakup spesifikasi sistem, penggunaan deret waktu atau data performa, koneksi jaringan, dan data proses. Anda dapat menggunakan informasi ini untuk memetakan aset IT Anda dan dependensi jaringannya. Semua titik data ini dapat membantu Anda menentukan biaya menjalankan server ini AWS dan juga merencanakan migrasi.

Data ditransmisikan dengan aman oleh Discovery Agent ke Application Discovery Service menggunakan enkripsi Keamanan Lapisan Pengangkutan (TLS). Agen dikonfigurasi untuk meng-

upgrade secara otomatis ketika versi baru tersedia. Anda dapat mengubah pengaturan konfigurasi ini jika diinginkan.

> **Tip**
>
> Sebelum mengunduh dan memulai penginstalan Discovery Agent, pastikan untuk membaca semua prasyarat yang diperlukan di Prasyarat untuk Agen Penemuan

Data yang dikumpulkan oleh Discovery Agent

AWS Application Discovery Agent (Discovery Agent) adalah perangkat lunak yang Anda instal di server lokal dan VMs. Discovery Agent mengumpulkan konfigurasi sistem, pemanfaatan seri waktu atau data kinerja, data proses, dan koneksi jaringan Transmission Control Protocol (TCP). Bagian ini menjelaskan data yang dikumpulkan.

Keterangan tabel untuk data yang dikumpulkan Discovery Agent:

- Istilah host mengacu pada server fisik atau VM.
- Data yang dikumpulkan adalah dalam pengukuran kilobyte (KB) kecuali dinyatakan lain.
- Data setara di konsol Migration Hub dilaporkan dalam megabyte (MB).
- Periode pemungutan suara dalam interval sekitar 15 detik dan dikirim ke AWS setiap 15 menit.
- Bidang data yang dilambangkan dengan tanda bintang (*) hanya tersedia dalam `.csv` file yang dihasilkan dari fungsi ekspor API agen.

Bidang data	Deskripsi
agentAssignedProcess[Id*]	ID proses dari proses yang ditemukan oleh agen
agentId	ID unik dari agen
agentProvidedTime[Stempel *]	Tanggal dan waktu observasi agen (mm/dd/yyyy hh:mm:ss am/pm)
cmdLine[*]	Proses yang dimasukkan pada baris perintah

Bidang data	Deskripsi
cpuType	Jenis CPU (unit pemrosesan pusat) yang digunakan dalam host
destinationIp*	Alamat IP perangkat yang menjadi tujuan pengiriman paket
destinationPort*	Nomor port data/request yang akan dikirim
family*	Protokol keluarga routing
freeRAM (MB)	RAM gratis dan RAM cache yang dapat dibuat dengan cepat dan tersedia untuk aplikasi, diukur dalam MB
gateway*	Alamat simpul jaringan
hostName	Nama data host yang dikumpulkan
hypervisor	Jenis hypervisor
ipAddress	Alamat IP host
ipVersion*	Nomor versi IP
isSystem*	Atribut Boolean untuk menunjukkan apakah proses dimiliki oleh OS
macAddress	Alamat MAC host
nama*	Nama data host, jaringan, metrik, dll yang sedang dikumpulkan
netMask*	Prefiks alamat IP yang dimiliki oleh host jaringan
osName	Nama sistem operasi pada host
osVersion	Versi sistem operasi pada host

Bidang data	Deskripsi
path	Jalur perintah yang bersumber dari baris perintah
sourceIp*	Alamat IP perangkat yang mengirim paket IP
sourcePort*	Nomor port dari mana data/request asalnya
stempel waktu*	Tanggal dan waktu atribut yang dilaporkan yang dicatat oleh agen
totalCpuUsagePct	Persentase penggunaan CPU pada host selama periode polling
totalDiskBytesReadPerSecond (Kbps)	Total kilobit dibaca per detik di semua disk
totalDiskBytesWrittenPerSecond (Kbps)	Total kilobit yang ditulis per detik di semua disk
totalDiskFreeUkuran (GB)	Ruang disk kosong yang dinyatakan dalam GB
totalDiskReadOpsPerSecond	Jumlah total I/O operasi baca per detik
totalDiskSize (GB)	Total kapasitas disk yang dinyatakan dalam GB
totalDiskWriteOpsPerSecond	Jumlah total I/O operasi tulis per detik
totalNetworkBytesReadPerSecond (Kbps)	Jumlah total throughput byte yang dibaca per detik
totalNetworkBytesWrittenPerSecond (Kbps)	Jumlah total throughput byte yang ditulis per detik
totalNumCores	Jumlah total unit pemrosesan independen dalam CPU
totalNumCpus	Jumlah total unit pemrosesan pusat
totalNumDisks	Jumlah hard disk fisik pada host

Bidang data	Deskripsi
totalNumLogical Prosesor*	Jumlah total inti fisik dikalikan jumlah utas yang dapat berjalan pada setiap inti
totalNumNetworkKartu	Jumlah total kartu jaringan pada server
totalRAM (MB)	Total jumlah RAM yang tersedia di host
transportProtocol*	Jenis protokol transport yang digunakan

Prasyarat untuk Agen Penemuan

Berikut ini adalah prasyarat dan tugas yang harus Anda lakukan sebelum Anda berhasil menginstal AWS Application Discovery Agent (Discovery Agent).

- Anda harus menetapkan wilayah AWS Migration Hub asal sebelum Anda mulai menginstal Discovery Agent.
- Jika agen versi 1.x terinstal, versi tersebut harus dihapus sebelum menginstal versi terbaru.
- Jika host tempat agen sedang diinstal menjalankan Linux, verifikasi bahwa host setidaknya mendukung arsitektur CPU Intel i686 (juga dikenal sebagai arsitektur mikro P6).
- Hasilkan kunci akses yang diperlukan untuk menginstal Discovery Agent.
- 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, 15 SP5

  Windows

  Windows Server 2003 R2 SP2

  Windows Server 2008 R1 SP2, 2008 R2 SP1

  Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- Jika koneksi keluar dari jaringan dibatasi, Anda harus memperbarui pengaturan firewall. Agen memerlukan akses ke `arsenal` melalui TCP port 443. Agen tidak memerlukan port masuk agar terbuka.

  Misalnya, jika wilayah asal Andaeu-`central-1`, Anda akan menggunakan `https://arsenal-discovery.`*`eu-central-1`*`.amazonaws.com:443`
- Akses ke Amazon S3 di wilayah asal Anda diperlukan agar peningkatan otomatis berfungsi.
- Buat pengguna AWS Identity and Access Management (IAM) di konsol dan lampirkan kebijakan terkelola `AWSApplicationDiscoveryAgentAccess` IAM yang ada. Kebijakan ini memungkinkan pengguna untuk melakukan tindakan agen yang diperlukan atas nama Anda. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.
- Periksa waktu yang miring dari server Network Time Protocol (NTP) Anda dan perbaiki jika diperlukan. Sinkronisasi waktu yang salah menyebabkan panggilan registrasi agen gagal.

> **Note**
>
> Discovery Agent memiliki agen 32-bit yang dapat dieksekusi, yang berfungsi pada sistem operasi 32-bit dan 64-bit. Jumlah paket instalasi yang diperlukan untuk deployment dikurangi dengan memiliki satu agen yang dapat dieksekusi. Agen yang dapat dieksekusi ini berfungsi untuk Linux dan OS Windows. Hal ini dibahas di bagian instalasi masing-masing yang mengikuti.

Instalasi Discovery Agent

Halaman ini mencakup cara menginstal Discovery Agent di Linux dan Microsoft Windows.

Instal Discovery Agent di Linux

Selesaikan prosedur berikut di Linux. Pastikan bahwa wilayah asal Migration Hub Anda telah ditetapkan sebelum memulai prosedur ini.

> **Note**
>
> Jika Anda menggunakan versi Linux yang tidak ada saat ini, lihat Pertimbangan dengan platform Linux yang lebih lama.

Untuk menginstal AWS Application Discovery Agent di pusat data Anda

1. Masuk ke server atau VM berbasis Linux Anda dan buat direktori baru untuk berisi komponen agen Anda.
2. Beralih ke direktori baru dan unduh skrip penginstalan dari baris perintah atau konsol.

   a. Untuk mengunduh dari baris perintah, jalankan perintah berikut.

   ```
   curl -o ./aws-discovery-agent.tar.gz https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
   ```

   b. Untuk mengunduh dari konsol Migration Hub, lakukan hal berikut:

      i. Masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.

      ii. Di halaman navigasi kiri, di bawah Temukan, pilih Alat.

      iii. Di kotak AWS Discovery Agent, pilih Download agents, lalu pilih Download for Linux. Unduhan Anda segera dimulai.

3. Verifikasi tanda tangan kriptografi paket instalasi dengan tiga perintah berikut:

   ```
   curl -o ./agent.sig https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz.sig
   ```

   ```
   curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/discovery.gpg
   ```

   ```
   gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
   ```

   Sidik jari kunci publik agen (`discovery.gpg`) adalah `7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2`.

4. Ekstrak dari tarball seperti yang ditunjukkan berikut ini.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Untuk menginstal agen, pilih salah satu metode instalasi berikut.

Untuk…	Melakukan ini...
Menginstal Discovery Agent	Untuk menginstal agen, jalankan perintah instal agen seperti yang ditunjukkan pada contoh berikut. Dalam contoh, ganti *your-home-region* dengan nama wilayah asal Anda, *aws-access-key-id* dengan access key ID Anda, dan *aws-secret-access-key* dengan secret access key Anda. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key` Secara default, agen secara otomatis mengunduh dan menerapkan pembaruan ketika sudah tersedia. Sebaiknya gunakan konfigurasi default ini. Namun, jika Anda tidak ingin agen mengunduh dan menerapkan pembaruan secara otomatis, sertakan parameter `-u false` ketika menjalankan perintah instal agen.
(Opsional) Instal Discovery Agent dan konfigurasikan proksi nontransparan	Untuk mengonfigurasi proksi nontransparan, tambahkan parameter berikut ke perintah instal agen: • -e Kata sandi proksi.

Untuk…	Melakukan ini...
	• -f Nomor port proksi. • -g Skema proksi. • -i Nama pengguna proksi. Berikut ini adalah contoh dari perintah instal agen menggunakan parameter proksi nontransparan. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` Jika proksi Anda tidak memerlukan autentikasi, tinggalkan parameter `-e` dan `-i`. Contoh perintah instal menggunakan `https`, jika proksi Anda menggunakan HTTP, tentukan `http` untuk nilai parameter `-g`.

6. Jika koneksi keluar dari jaringan dibatasi, Anda harus memperbarui pengaturan firewall. Agen memerlukan akses ke `arsenal` melalui TCP port 443. Agen tidak memerlukan port masuk agar terbuka.

   Misalnya, jika wilayah asal Anda`eu-central-1`, Anda akan menggunakan `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Pertimbangan dengan platform Linux yang lebih lama

Beberapa platform Linux lama seperti SUSE 10, CentOS 5, dan RHEL 5 berada di akhir masa pakai atau hanya didukung secara minimal. Platform ini dapat menderita out-of-date cipher suite yang mencegah skrip pembaruan agen mengunduh paket instalasi.

Curl

Agen Application Discovery membutuhkan `curl` komunikasi yang aman dengan AWS server. Beberapa versi lama `curl` tidak dapat berkomunikasi dengan aman dengan layanan web modern.

Untuk menggunakan versi `curl` yang disertakan dengan agen Application Discovery untuk semua operasi, jalankan skrip instalasi dengan parameter `-c true`.

Paket Otoritas Sertifikasi

Sistem Linux yang lebih lama mungkin memiliki bundel out-of-date Certificate Authority (CA), yang sangat penting untuk mengamankan komunikasi internet.

Untuk menggunakan paket CA yang disertakan dengan agen Application Discovery untuk semua operasi, jalankan skrip instalasi dengan parameter `-b true`.

Opsi skrip instalasi ini dapat digunakan bersama. Dalam contoh perintah berikut, kedua parameter skrip diteruskan ke skrip instalasi:

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c
 true -b true
```

Instal Discovery Agent di Microsoft Windows

Selesaikan prosedur berikut untuk menginstal agen di Microsoft Windows. Pastikan bahwa wilayah asal Migration Hub Anda telah ditetapkan sebelum memulai prosedur ini.

Untuk menginstal AWS Application Discovery Agent di pusat data Anda

1. Unduh Penginstal agen Windows tapi jangan diklik dua kali untuk menjalankan penginstal dalam Windows.

   > **Important**
   >
   > Jangan klik dua kali untuk menjalankan penginstal dalam Windows karena akan gagal untuk menginstal. Penginstalan agen hanya berfungsi dari prompt perintah. (Jika Anda sudah mengeklik dua kali pada penginstal, Anda mesti membuka Tambah/Hapus

Program dan menghapus instalasi agen sebelum melanjutkan langkah-langkah instalasi yang tersisa.)
Jika penginstal agen Windows tidak mendeteksi versi apa pun dari runtime Visual C++ x86 pada host, secara otomatis menginstal runtime Visual C++ x86 2015—2019 sebelum menginstal perangkat lunak agen.

2. Buka prompt perintah sebagai administrator dan arahkan ke lokasi di mana Anda menyimpan paket instalasi.
3. Untuk menginstal agen, pilih salah satu metode instalasi berikut.

Untuk…	Melakukan ini...
Menginstal Discovery Agent	Untuk menginstal agen, jalankan perintah instal agen seperti yang ditunjukkan pada contoh berikut. Dalam contoh, ganti *your-home-region* dengan nama wilayah asal Anda, *aws-access-key-id* dengan ID kunci akses Anda, dan *aws-secret-access-key* dengan kunci akses rahasia Anda. Opsional, Anda dapat mengatur lokasi instalasi agen dengan menentukan lintasan folder *C:\install-location* untuk parameter LOKASIINSTALASI. Misalnya, `INSTALLLOCATION="` *C:\install-location* `"`. Hirarki folder yang dihasilkan adalah [jalur INSTALLLOCATION]\AWS Discovery. Secara default, lokasi instalasi adalah folder `Program Files`. Secara opsional, Anda dapat menggunakan `LOGANDCONFIGLOCATION` untuk mengganti direktori default (ProgramData) untuk folder log agen dan file konfigurasi. Hirarki folder yang dihasilka

Untuk…	Melakukan ini...
	n adalah [*LOGANDCONFIGLOCATION path*]\AWS Discovery . `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " /quiet` Secara default, agen secara otomatis mengunduh dan menerapkan pembaruan ketika sudah tersedia. Sebaiknya gunakan konfigurasi default ini. Namun, jika Anda tidak ingin agen mengunduh dan menerapkan pembaruan secara otomatis, sertakan parameter berikut ketika menjalankan perintah instal agen: `AUTO_UPDATE=false` **Warning** Menonaktifkan peningkatan otomatis akan mencegah patch keamanan terbaru diinstal.

Untuk…	Melakukan ini...
(Opsional) Instal Discovery Agent dan konfigurasikan proksi nontransparan	Untuk mengonfigurasi proksi nontransparan, tambahkan properti publik berikut untuk perintah instal agen: • PROXY_HOST — Nama host proxy • PROXY_SCHEME — Skema proxy • PROXY_PORT — Nomor port proxy • PROXY_USER — Nama pengguna proxy • PROXY_PASSWORD — Kata sandi pengguna proxy Berikut ini adalah contoh dari perintah instal agen menggunakan properti proksi nontransparan. `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` Jika proxy Anda tidak memerlukan otentikasi, maka hilangkan properti `PROXY_USER` dan`PROXY_PASSWORD` . Contoh perintah install menggunakan`https`. Jika proxy Anda menggunakan HTTP, `http` tentukan `PROXY_SCHEME` nilainya.

4. Jika koneksi keluar dari jaringan Anda dibatasi, Anda harus memperbarui pengaturan firewall Anda. Agen memerlukan akses ke `arsenal` melalui TCP port 443. Agen tidak memerlukan port masuk agar terbuka.

Misalnya, jika Wilayah asal Andaeu-central-1, Anda akan menggunakan yang berikut ini: `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Package sign dan upgrade otomatis

Untuk Windows Server 2008 dan yang lebih baru, Amazon secara kriptografis menandatangani paket instalasi agen Application Discovery Service dengan sertifikat SHA256 . Untuk autoupdates yang SHA2 ditandatangani pada Windows Server 2008 SP2, pastikan bahwa host memiliki hotfix yang diinstal untuk mendukung otentikasi tanda tangan. SHA2 Hotfix dukungan terbaru Microsoft membantu mendukung SHA2 otentikasi pada Windows Server 2008. SP2

> **Note**
>
> Hotfix untuk SHA256 dukungan untuk Windows 2003 tidak lagi tersedia untuk umum dari Microsoft. Jika perbaikan ini belum diinstal di host Windows 2003 Anda, upgrade manual diperlukan.

Untuk melakukan upgrade secara manual

1. Unduh Windows Agent Updater.
2. Buka command prompt sebagai administrator.
3. Arahkan ke lokasi tempat pembaru disimpan.
4. Jalankan perintah berikut.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Mengelola proses Discovery Agent

Halaman ini mencakup cara mengelola Discovery Agent di Linux dan Microsoft Windows.

Kelola proses Discovery Agent di Linux

Anda dapat mengelola perilaku Discovery Agent di tingkat sistem menggunakan alat `systemd`, `Upstart`, atau `System V init`. Tab berikut menguraikan perintah untuk tugas yang didukung di setiap alat.

systemd

Perintah Manajemen untuk Application Discovery Agent

Tugas	Perintah
Verifikasi bahwa agen sedang berjalan	`sudo systemctl status aws-discovery-daemon.service`
Mulai agen	`sudo systemctl start aws-discovery-daemon.service`
Hentikan agen	`sudo systemctl stop aws-discovery-daemon.service`
Mulai ulang agen	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

Perintah manajemen untuk Agen Penemuan Aplikasi

Tugas	Perintah
Verifikasi bahwa agen sedang berjalan	`sudo initctl status aws-discovery-daemon`
Mulai agen	`sudo initctl start aws-discovery-daemon`
Hentikan agen	`sudo initctl stop aws-discovery-daemon`
Mulai ulang agen	`sudo initctl restart aws-discovery-daemon`

System V init

Perintah manajemen untuk Agen Penemuan Aplikasi

Tugas	Perintah
Verifikasi bahwa agen sedang berjalan	`sudo /etc/init.d/aws-discovery-daemon status`
Mulai agen	`sudo /etc/init.d/aws-discovery-daemon start`
Hentikan agen	`sudo /etc/init.d/aws-discovery-daemon stop`
Mulai ulang agen	`sudo /etc/init.d/aws-discovery-daemon restart`

Kelola proses Discovery Agent di Microsoft Windows

Anda dapat mengelola perilaku Discovery Agent di tingkat sistem melalui konsol Layanan Pengelola Server Windows. Tabel berikut menjelaskan caranya.

Tugas	Nama Layanan	Status/Tindakan Layanan
Verifikasi bahwa agen sedang berjalan	AWS Agen Penemuan AWS Pembaru Penemuan	Dimulai
Mulai agen	AWS Agen Penemuan AWS Pembaru Penemuan	Pilih Mulai
Hentikan agen	AWS Agen Penemuan AWS Pembaru Penemuan	Pilih Berhenti
Mulai ulang agen	AWS Agen Penemuan AWS Pembaru Penemuan	Pilih Mulai Ulang

Menghapus Instalasi Discovery Agent

Halaman ini mencakup cara menghapus Discovery Agent di Linux dan Microsoft Windows.

Menghapus Instalasi Discovery Agent di Linux

Bagian ini menjelaskan cara menghapus instalasi Discovery Agent di Linux.

Untuk menghapus instalasi agen jika Anda menggunakan pengelola paket yum

- Gunakan perintah berikut untuk menghapus instalasi agen jika menggunakan yum.

```
rpm -e --nodeps aws-discovery-agent
```

Untuk menghapus instalasi agen jika Anda menggunakan pengelola paket apt-get

- Gunakan perintah berikut untuk menghapus instalasi agen jika menggunakan apt-get.

```
apt-get remove aws-discovery-agent:i386
```

Untuk menghapus instalasi agen jika Anda menggunakan pengelola paket zypper

- Gunakan perintah berikut untuk menghapus instalasi agen jika menggunakan zypper.

```
zypper remove aws-discovery-agent
```

Copot pemasangan Discovery Agent di Microsoft Windows

Bagian ini menjelaskan cara menghapus Discovery Agent di Microsoft Windows.

Untuk menghapus instalasi Discovery Agent pada Windows

1. Buka Control Panel di Windows.
2. Pilih Program.
3. Pilih Program dan Fitur.
4. Pilih AWS Discovery Agent.

5. Pilih Hapus Instalasi.

> **Note**
>
> Jika Anda memilih untuk menginstal ulang agen setelah mencopotnya, jalankan perintah berikut dengan opsi `/repair` dan`/norestart`.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
> ```

Untuk menghapus instalan agen penemuan di Windows menggunakan baris perintah

1. Klik kanan Mulai.
2. Pilih Command Prompt.
3. Gunakan perintah berikut untuk menghapus instalan agen penemuan di Windows.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

> **Note**
>
> Jika `.exe` file ada di server, Anda dapat menghapus instalan agen sepenuhnya dari server dengan menggunakan perintah berikut. Jika Anda menggunakan perintah ini untuk menghapus instalan, Anda tidak perlu menggunakan `/norestart` opsi `/repair` dan saat menginstal ulang agen.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

Memulai dan menghentikan pengumpulan data Discovery Agent

Setelah Discovery Agent dideploy dan dikonfigurasi, jika pengumpulan data berhenti, Anda dapat memulai ulang. Anda dapat memulai atau menghentikan pengumpulan data melalui konsol dengan mengikuti langkah-langkahMemulai dan menghentikan pengumpul data di konsol AWS Migration

Hub, atau dengan melakukan panggilan API melalui AWS CLI. Sebelum memulai pastikan untuk menghasilkan kunci akses yang diperlukan untuk mengelola Agen Penemuan.

Untuk menginstal AWS CLI dan memulai atau menghentikan pengumpulan data

1. Jika Anda belum melakukannya, instal yang AWS CLI sesuai dengan jenis OS Anda (Windows atau Mac/Linux). Lihat Panduan Pengguna AWS Command Line Interface untuk instruksi.
2. Buka Command prompt (Windows) atau Terminal (MAC/Linux).
   a. Ketik `aws configure` dan tekan Enter.
   b. Masukkan ID Kunci AWS Akses dan Kunci Akses AWS Rahasia Anda.
   c. Masukkan Wilayah rumah Anda untuk Nama Wilayah Default, misalnya*us-west-2*. (Kami berasumsi bahwa itu `us-west-2` adalah Wilayah asal Anda dalam contoh ini.)
   d. Masukkan `text` untuk Format Output Default.
3. Untuk menemukan ID agen yang ingin Anda hentikan atau mulai pengumpulan datanya, ketik perintah berikut:

```
aws discovery describe-agents
```

4. Untuk memulai pengumpulan data oleh agen, ketik perintah berikut ini:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

   Untuk menghentikan pengumpulan data oleh agen, ketik perintah berikut ini:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Pemecahan Masalah Agen Penemuan

Halaman ini mencakup pemecahan masalah Discovery Agent di Linux dan Microsoft Windows.

Memecahkan Masalah Agen Penemuan di Linux

Jika Anda mengalami masalah saat menginstal atau menggunakan Discovery Agent di Linux, baca panduan berikut tentang pencatatan dan konfigurasi. Saat membantu memecahkan masalah

potensial dengan agen atau koneksinya ke Application Discovery Service, AWS Support sering meminta file-file ini.

- File log

  Berkas log untuk Discovery Agent terletak di direktori berikut.

  ```
  /var/log/aws/discovery/
  ```

  Berkas log diberi nama untuk menunjukkan apakah mereka dihasilkan oleh daemon utama, peng-upgrade otomatis, atau penginstal.

- File konfigurasi

  File konfigurasi untuk Discovery Agent versi 2.0.1617.0 atau yang lebih baru terletak di direktori berikut.

  ```
  /etc/opt/aws/discovery/
  ```

  File konfigurasi untuk Discovery Agent versi sebelum 2.0.1617.0 terletak di direktori berikut.

  ```
  /var/opt/aws/discovery/
  ```

- Untuk petunjuk tentang cara menghapus versi lama Discovery Agent, lihat Prasyarat untuk Agen Penemuan.

Memecahkan Masalah Agen Penemuan di Microsoft Windows

Jika Anda mengalami masalah saat menginstal atau menggunakan Agen Penemuan AWS Aplikasi di Microsoft Windows, baca panduan berikut tentang pencatatan dan konfigurasi. AWS Dukungan sering meminta file-file ini ketika membantu memecahkan masalah potensial dengan agen atau hubungannya ke Application Discovery Service.

- Pencatatan instalasi

  Dalam beberapa kasus, perintah agent install tampaknya gagal. Sebagai contoh, kegagalan dapat muncul dengan Windows Services Manager yang menunjukkan bahwa layanan penemuan

tidak sedang dibuat. Dalam hal ini, tambahkan /log install.log ke perintah untuk menghasilkan log instalasi verbose.

- Penebangan operasional

  Pada Windows Server 2008 dan yang lebih baru, berkas log agen dapat ditemukan di bawah direktori berikut.

  ```
  C:\ProgramData\AWS\AWS Discovery\Logs
  ```

  Pada Windows Server 2003, berkas log agen dapat ditemukan di bawah direktori berikut.

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
  ```

  File log diberi nama untuk menunjukkan apakah dihasilkan oleh layanan utama, peningkatan otomatis, atau penginstal.

- File konfigurasi

  Pada Windows Server 2008 dan yang lebih baru, file konfigurasi agen dapat ditemukan di lokasi berikut.

  ```
  C:\ProgramData\AWS\AWS Discovery\config
  ```

  Pada Windows Server 2003, file konfigurasi agen dapat ditemukan di lokasi berikut.

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
  ```

- Untuk petunjuk tentang cara menghapus versi Discovery Agent sebelumnya, lihatPrasyarat untuk Agen Penemuan.

Application Discovery Service Agentless Collector

Application Discovery Service Agentless Collector (Agentless Collector) adalah aplikasi lokal yang mengumpulkan informasi melalui metode tanpa agen tentang lingkungan lokal Anda, termasuk informasi profil server (misalnya, OS, jumlah, jumlah RAM), metadata database, metrik pemanfaatan, dan data tentang lalu lintas jaringan di antara server lokal. CPUs Anda menginstal Agentless Collector sebagai mesin virtual (VM) di lingkungan Server VMware vCenter Anda menggunakan file Open Virtualization Archive (OVA).

Agentless Collector memiliki arsitektur modular, yang memungkinkan penggunaan beberapa metode pengumpulan tanpa agen. Agentless Collector menyediakan modul untuk pengumpulan data dari VMware VMs dan dari database dan server analitik. Ini juga menyediakan modul untuk mengumpulkan data tentang lalu lintas jaringan di antara server lokal Anda.

Agentless Collector mendukung pengumpulan data untuk AWS Application Discovery Service (Application Discovery Service) dengan mengumpulkan data penggunaan dan konfigurasi tentang server dan database lokal Anda, serta data tentang lalu lintas jaringan di antara server lokal Anda.

Application Discovery Service terintegrasi dengan AWS Migration Hub, layanan yang menyederhanakan pelacakan migrasi Anda saat menggabungkan informasi status migrasi Anda ke dalam satu konsol. Anda dapat melihat server yang ditemukan, mendapatkan rekomendasi Amazon EC2, memvisualisasikan koneksi jaringan, mengelompokkan server ke dalam aplikasi, lalu melacak status migrasi setiap aplikasi dari konsol Hub Migrasi di Wilayah asal Anda.

Database Agentless Collector dan modul pengumpulan data analitik terintegrasi dengan AWS Database Migration Service ()AWS DMS. Integrasi ini membantu merencanakan migrasi Anda ke AWS Cloud. Anda dapat menggunakan modul pengumpulan data database dan analitik untuk menemukan server database dan analitik di lingkungan Anda dan membangun inventaris server yang ingin Anda migrasikan ke AWS Cloud. Modul pengumpulan data ini mengumpulkan metadata database dan metrik pemanfaatan aktual CPU, memori, dan kapasitas disk. Setelah mengumpulkan metrik ini, Anda dapat menggunakan AWS DMS konsol untuk menghasilkan rekomendasi target untuk basis data sumber Anda.

Prasyarat untuk Kolektor Tanpa Agen

Berikut ini adalah prasyarat untuk menggunakan Application Discovery Service Agentless Collector (Agentless Collector):

- Satu atau lebih AWS akun.
- AWS Akun dengan set Wilayah AWS Migration Hub asal, lihatMasuk ke konsol Migration Hub dan pilih Wilayah beranda. Data Hub Migrasi Anda disimpan di Wilayah asal Anda untuk tujuan penemuan, perencanaan, dan pelacakan migrasi.
- Pengguna IAM AWS akun yang disiapkan untuk menggunakan kebijakan AWS `AWSApplicationDiscoveryAgentlessCollectorAccess` terkelola. Untuk menggunakan modul pengumpulan data database dan analitik, pengguna IAM ini juga harus menggunakan dua kebijakan `DMSCollectorPolicy` IAM yang dikelola pelanggan dan. `FleetAdvisorS3Policy` Untuk informasi selengkapnya, lihat Menyebarkan Application Discovery Service Agentless Collector. Pengguna IAM harus dibuat di AWS akun dengan set Wilayah beranda Migration Hub.
- VMware vCenter Server V5.5, V6, V6.5, 6.7 atau 7.0.

> **Note**
>
> Agentless Collector mendukung semua versi ini VMware, tetapi saat ini kami menguji terhadap versi 6.7 dan 7.0.

- Untuk penyiapan VMware VCenter Server, pastikan Anda dapat memberikan kredensyal vCenter dengan izin Baca dan Lihat yang ditetapkan untuk grup Sistem.
- Agentless Collector memerlukan akses keluar melalui port TCP 443 ke beberapa domain. AWS Untuk daftar domain ini, lihatKonfigurasikan firewall untuk akses keluar ke domain AWS.
- Untuk menggunakan modul pengumpulan data database dan analitik, buat bucket Amazon S3 di tempat Wilayah AWS yang Anda tetapkan sebagai Wilayah beranda Hub Migrasi. Modul pengumpulan data database dan analitik menyimpan metadata inventaris di bucket Amazon S3 ini. Lihat informasi yang lebih lengkap di Membuat bucket dalam Panduan Pengguna Amazon S3.
- Agentless Collector versi 2 membutuhkan ESXi 6.5 atau versi yang lebih baru.

Konfigurasikan perimeter data untuk akses ke sumber daya milik layanan AWS

Fitur pembaruan otomatis Agentless Collector mengambil pembaruan dalam bentuk gambar Docker dari Repositori ECR Publik milik AWS layanan. Jika Anda menggunakan perimeter data untuk mengontrol akses ke Amazon ECR di lingkungan Anda, Anda mungkin perlu secara eksplisit mengizinkan akses ke hal-hal berikut untuk menggunakan fitur pembaruan otomatis:

- Sumber daya ARNs yang membutuhkan akses: `arn:aws:ecr-public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b`
- Izin yang diperlukan: `ecr-public:DescribeImages`

Konfigurasikan firewall untuk akses keluar ke domain AWS

Jika koneksi keluar dari jaringan Anda dibatasi, Anda harus memperbarui pengaturan firewall Anda untuk memungkinkan akses keluar ke AWS domain yang diperlukan oleh Agentless Collector. AWS Domain mana yang memerlukan akses keluar bergantung pada apakah Wilayah asal Hub Migrasi Anda adalah Wilayah AS Barat (Oregon), us-west-2, atau Wilayah lainnya.

Domain berikut memerlukan akses keluar jika wilayah beranda AWS akun Anda adalah us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`— Kolektor menggunakan domain ini untuk memvalidasi bahwa domain tersebut dikonfigurasi dengan kredensyal pengguna IAM yang diperlukan. Kolektor juga menggunakannya untuk mengirim dan menyimpan data yang dikumpulkan karena Wilayah asal adalah us-west-2.
- `migrationhub-config.us-west-2.amazonaws.com`— Kolektor menggunakan domain ini untuk menentukan Wilayah rumah mana kolektor mengirimkan data berdasarkan kredensyal pengguna IAM yang disediakan.
- `api.ecr-public.us-east-1.amazonaws.com`— Kolektor menggunakan domain ini untuk menemukan pembaruan yang tersedia.
- `public.ecr.aws`— Kolektor menggunakan domain ini untuk mengunduh pembaruan.
- dms.*`your-migrationhub-home-region`*`.amazonaws.com`— Kolektor menggunakan domain ini untuk terhubung ke pengumpul AWS DMS data.
- `s3.amazonaws.com`— Kolektor menggunakan domain ini untuk mengunggah data yang dikumpulkan oleh database dan modul pengumpulan data analitik ke bucket Amazon S3 Anda.
- `sts.amazonaws.com`— Kolektor menggunakan domain ini untuk memahami akun apa yang telah dikonfigurasi oleh kolektor.

Domain berikut memerlukan akses keluar jika wilayah beranda AWS akun Anda tidak: **`us-west-2`**

- `arsenal-discovery.us-west-2.amazonaws.com`— Kolektor menggunakan domain ini untuk memvalidasi bahwa domain tersebut dikonfigurasi dengan kredensyal pengguna IAM yang diperlukan.

- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com`— Kolektor menggunakan domain ini untuk mengirim dan menyimpan data yang dikumpulkan.
- `migrationhub-config.us-west-2.amazonaws.com`— Kolektor menggunakan domain ini untuk menentukan Wilayah rumah mana kolektor harus mengirim data berdasarkan kredensi pengguna IAM yang disediakan.
- `api.ecr-public.us-east-1.amazonaws.com`— Kolektor menggunakan domain ini untuk menemukan pembaruan yang tersedia.
- `public.ecr.aws`— Kolektor menggunakan domain ini untuk mengunduh pembaruan.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— Kolektor menggunakan domain ini untuk terhubung ke pengumpul AWS DMS data.
- `s3.amazonaws.com`— Kolektor menggunakan domain ini untuk mengunggah data yang dikumpulkan oleh database dan modul pengumpulan data analitik ke bucket Amazon S3 Anda.
- `sts.amazonaws.com`— Kolektor menggunakan domain ini untuk memahami akun apa yang telah dikonfigurasi oleh kolektor.

Saat menyiapkan Kolektor Tanpa Agen, Anda mungkin menerima kesalahan seperti Penyiapan gagal — Periksa kredensialnya dan coba lagi atau AWS tidak dapat dihubungi. Harap verifikasi pengaturan jaringan. Kesalahan ini dapat disebabkan oleh upaya yang gagal oleh Agentless Collector untuk membuat koneksi HTTPS ke salah satu AWS domain yang memerlukan akses keluar.

Jika sambungan ke AWS tidak dapat dibuat, Agentless Collector tidak dapat mengumpulkan data dari lingkungan lokal Anda. Untuk informasi tentang cara memperbaiki koneksi ke AWS, lihatMemperbaiki Agentless Collector tidak dapat mencapai AWS selama pengaturan.

Menyebarkan Application Discovery Service Agentless Collector

Untuk menggunakan Application Discovery Service Agentless Collector, Anda harus terlebih dahulu membuat pengguna IAM dan mengunduh kolektor. Halaman ini memandu Anda melalui langkah-langkah yang harus diambil untuk menyebarkan kolektor.

Buat pengguna IAM untuk Agentless Collector

Untuk menggunakan Agentless Collector, di AWS akun yang Anda gunakanMasuk ke konsol Migration Hub dan pilih Wilayah beranda, Anda harus membuat pengguna AWS Identity and Access Management (IAM). Kemudian, siapkan pengguna IAM ini untuk menggunakan kebijakan AWS

AWSApplicationDiscoveryAgentlessCollectorAccessterkelola berikut. Anda melampirkan kebijakan IAM ini saat Anda membuat pengguna IAM.

Untuk menggunakan modul pengumpulan data database dan analitik, buat dua kebijakan IAM yang dikelola pelanggan. Kebijakan ini menyediakan akses bucket Amazon S3 dan API Anda. AWS DMS Untuk informasi selengkapnya, lihat Membuat kebijakan terkelola pelanggan di Panduan Pengguna IAM.

- Gunakan kode JSON berikut untuk membuat **`DMSCollectorPolicy`** kebijakan.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "dms:DescribeFleetAdvisorCollectors",
            "dms:ModifyFleetAdvisorCollectorStatuses",
            "dms:UploadFileMetadataList"
        ],
        "Resource": "*"
    }]
}
```

- Gunakan kode JSON berikut untuk membuat **`FleetAdvisorS3Policy`** kebijakan.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:GetBucket*",
                "s3:List*",
                "s3:DeleteObject*",
                "s3:PutObject*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
```

```
                "arn:aws:s3:::bucket_name/*"
            ]
        }
    ]
}
```

Pada contoh sebelumnya, ganti *bucket_name* dengan nama bucket Amazon S3 yang Anda buat di langkah prasyarat.

Kami menyarankan Anda membuat pengguna IAM non-administratif untuk digunakan dengan Agentless Collector. Saat membuat pengguna IAM non-administratif, ikuti praktik terbaik keamanan dengan Berikan Hak Istimewa Minimum, untuk memberikan izin minimum kepada pengguna.

Untuk membuat pengguna IAM non-administrator untuk digunakan dengan Agentless Collector

1. Masuk Konsol Manajemen AWS, navigasikan ke konsol IAM, menggunakan AWS akun yang Anda gunakan untuk mengatur Wilayah Masuk ke konsol Migration Hub dan pilih Wilayah beranda beranda.
2. Buat pengguna IAM non-administrator dengan mengikuti petunjuk untuk membuat pengguna dengan konsol seperti yang dijelaskan dalam Membuat pengguna IAM di AWS akun Anda di Panduan Pengguna IAM.

   Sambil mengikuti petunjuk dalam Panduan Pengguna IAM:

   - Ketika pada langkah tentang memilih jenis akses, pilih Akses terprogram. Catatan, meskipun tidak disarankan, hanya pilih akses AWS Management Console jika Anda berencana menggunakan kredenal pengguna IAM yang sama untuk mengakses konsol. AWS
   - Saat berada di langkah tentang halaman Setel izin, pilih opsi untuk Melampirkan kebijakan yang ada ke pengguna secara langsung. Kemudian pilih kebijakan `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS terkelola dari daftar kebijakan.

     Selanjutnya, pilih kebijakan IAM `DMSCollectorPolicy` dan yang dikelola `FleetAdvisorS3Policy` pelanggan.
   - Ketika pada langkah tentang melihat kunci akses pengguna (kunci akses IDs dan kunci akses rahasia), ikuti panduan di Catatan penting tentang menyimpan ID kunci akses baru pengguna dan kunci akses rahasia di tempat yang aman dan terlindungi. Anda akan memerlukan kunci akses ini diMengkonfigurasi Kolektor Tanpa Agen.

Ini adalah praktik terbaik AWS keamanan untuk memutar kunci akses. Untuk informasi tentang memutar kunci, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang dalam Panduan Pengguna IAM.

Unduh Kolektor Tanpa Agen

Untuk mengatur Application Discovery Service Agentless Collector (Agentless Collector), Anda harus mengunduh dan menyebarkan file Agentless Collector Open Virtualization Archive (OVA). Agentless Collector adalah alat virtual yang Anda instal di lingkungan lokal VMware Anda. Langkah ini menjelaskan cara mengunduh file OVA kolektor dan langkah selanjutnya menjelaskan cara menerapkannya.

Untuk mengunduh file OVA kolektor dan memverifikasi checksum-nya

1. Masuk ke vCenter sebagai VMware administrator dan beralih ke direktori tempat Anda ingin mengunduh file OVA Agentless Collector.
2. Unduh file OVA dari URL berikut:

   OVA Kolektor Tanpa Agen
3. Bergantung pada algoritma hashing yang Anda gunakan di lingkungan sistem Anda, unduh file MD5atau SHA256untuk mendapatkan file yang berisi nilai checksum. Gunakan nilai yang diunduh untuk memverifikasi `ApplicationDiscoveryServiceAgentlessCollector` file yang diunduh pada langkah sebelumnya.
4. Bergantung pada variasi Linux Anda, jalankan MD5 perintah atau SHA256 perintah versi yang sesuai untuk memverifikasi bahwa tanda tangan kriptografi `ApplicationDiscoveryServiceAgentlessCollector.ova` file cocok dengan nilai di masing-masing MD5 SHA256 file/yang Anda unduh.

   ```
   $ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
   ```

   ```
   $ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
   ```

Menyebarkan Kolektor Tanpa Agen

Application Discovery Service Agentless Collector (Agentless Collector) adalah alat virtual yang Anda instal di lingkungan lokal Anda. VMware Bagian ini menjelaskan cara menyebarkan file Open Virtualization Archive (OVA) yang Anda unduh di lingkungan Anda VMware .

Spesifikasi mesin virtual Agentless Collector

Agentless Collector version 2

- Sistem Operasi - Amazon Linux 2023
- RAM - 16 GB
- CPU - 4 core
- VMware persyaratan - Lihat persyaratan VMware host untuk AL2023 menjalankan VMware

Agentless Collector version 1

- Sistem Operasi - Amazon Linux 2
- RAM - 16 GB
- CPU - 4 core

Prosedur berikut memberi Anda langkah melalui penerapan file OVA Agentless Collector di lingkungan Anda. VMware

Untuk menyebarkan Agentless Collector

1. Masuk ke vCenter sebagai administrator. VMware
2. Gunakan salah satu cara berikut untuk menginstal file OVA:
   - Gunakan UI: Pilih File, pilih Deploy OVF Template, pilih file OVA kolektor yang Anda unduh di bagian sebelumnya, lalu lengkapi wizard. Pastikan pengaturan proxy di dasbor manajemen server dikonfigurasi dengan benar.
   - Gunakan baris perintah: Untuk menginstal file OVA kolektor dari baris perintah, unduh dan gunakan Alat Format Virtualisasi VMware Terbuka (ovftool). Untuk mengunduh ovftool, pilih rilis dari halaman Dokumentasi Alat OVF.

     Berikut ini adalah contoh penggunaan alat baris perintah ovftool untuk menginstal file OVA kolektor.

```
ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1
 -dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova
 'vi://username:password@vcenterurl/Datacenter/host/esxi/'
```

Berikut ini menjelaskan ***replaceable*** nilai-nilai dalam contoh

- Nama adalah nama yang ingin Anda gunakan untuk VM Kolektor Tanpa Agen Anda.
- Datastore adalah nama datastore di vCenter Anda.
- Nama file OVA adalah nama file OVA kolektor yang diunduh.
- Itu username/password adalah kredensyal vCenter Anda.
- Vcenterurl adalah URL vCenter Anda.
- Jalur vi adalah jalan menuju VMware ESXi tuan rumah Anda.

3. Temukan Kolektor Tanpa Agen yang digunakan di vCenter Anda. Klik kanan VM, lalu pilih Power, Power On.
4. Setelah beberapa menit, alamat IP kolektor ditampilkan di vCenter. Anda menggunakan alamat IP ini untuk terhubung ke kolektor.

Mengakses konsol Agentless Collector

Prosedur berikut menjelaskan cara mengakses konsol Application Discovery Service Agentless Collector (Agentless Collector).

Untuk mengakses konsol Agentless Collector

1. Buka browser web, lalu ketik URL berikut di bilah alamat: **https://** *<ip_address>***/**, dari *<ip_address>* mana alamat IP kolektor berasalMenyebarkan Kolektor Tanpa Agen.
2. Pilih Memulai saat pertama kali Anda mengakses Agentless Collector. Setelah itu, Anda akan diminta untuk Login.

Jika Anda mengakses konsol Agentless Collector untuk pertama kalinya, selanjutnya Anda akan melakukannya. Mengkonfigurasi Kolektor Tanpa Agen Jika tidak, selanjutnya Anda akan melihatDasbor Kolektor Tanpa Agen.

Mengkonfigurasi Kolektor Tanpa Agen

Application Discovery Service Agentless Collector (Agentless Collector) adalah mesin virtual (VM) berbasis Amazon Linux 2. Bagian berikut menjelaskan cara mengonfigurasi VM kolektor di halaman Konfigurasi Kolektor Tanpa Agen Konfigurasi Kolektor Tanpa Agen.

Untuk mengkonfigurasi VM kolektor pada halaman Konfigurasi Kolektor Tanpa Agen

1. Untuk nama Kolektor, masukkan nama untuk kolektor untuk mengidentifikasinya. Nama dapat berisi spasi tetapi tidak dapat berisi karakter khusus.
2. Di bawah Sinkronisasi data, masukkan kunci AWS akses dan kunci rahasia untuk pengguna IAM AWS akun untuk menentukan sebagai akun tujuan untuk menerima data yang ditemukan oleh kolektor. Untuk informasi tentang persyaratan untuk pengguna IAM, lihatMenyebarkan Application Discovery Service Agentless Collector.

   a. Untuk AWS kunci akses, masukkan kunci akses pengguna IAM AWS akun yang Anda tentukan sebagai akun tujuan.

   b. Untuk AWS kunci rahasia, masukkan kunci rahasia pengguna IAM AWS akun yang Anda tentukan sebagai akun tujuan.

   c. (Opsional) Jika jaringan Anda memerlukan penggunaan proxy untuk mengakses AWS, masukkan host proxy, port proxy, dan, secara opsional, kredensi yang diperlukan untuk mengautentikasi dengan server proxy yang ada.
3. Di bawah kata sandi Agentless Collector, atur kata sandi yang akan digunakan untuk mengautentikasi akses ke Agentless Collector.

   - Kata sandi peka huruf besar/kecil
   - Kata sandi harus memiliki panjang antara 8 dan 64 karakter
   - Kata sandi harus mengandung setidaknya satu karakter dari masing-masing dari empat kategori berikut:
     - Huruf kecil (a-z)
     - Huruf besar (A-Z)
     - Angka (0-9)
     - Karakter non-alfanumerik (@ $! #%*? &)
   - Kata sandi tidak dapat berisi karakter khusus selain yang berikut: @$! #%*? &

a. Untuk kata sandi Agentless Collector, masukkan kata sandi yang akan digunakan untuk mengautentikasi akses ke kolektor.

b. Untuk Masukkan kembali kata sandi Agentless Collector, untuk verifikasi, masukkan kata sandi lagi.

4. Di bawah pengaturan lain, baca Perjanjian Lisensi. Jika Anda setuju untuk menerimanya, pilih kotak centang.
5. Untuk mengaktifkan pembaruan otomatis untuk Kolektor Tanpa Agen, di bawah Pengaturan lain, pilih Perbarui Kolektor Tanpa Agen secara otomatis. Jika Anda tidak memilih kotak centang ini, Anda harus memperbarui Agentless Collector secara manual seperti yang dijelaskan dalam. Memperbarui Application Discovery Service Agentless Collector secara manual
6. Pilih Simpan konfigurasi.

Topik berikut menjelaskan tugas konfigurasi kolektor opsional.

Tugas Konfigurasi Opsional

- (Opsional) Konfigurasikan alamat IP statis untuk VM Kolektor Tanpa Agen
- (Opsional) Setel ulang VM Kolektor Tanpa Agen kembali menggunakan DHCP
- (Opsional) Konfigurasikan protokol otentikasi Kerberos

(Opsional) Konfigurasikan alamat IP statis untuk VM Kolektor Tanpa Agen

Langkah-langkah berikut menjelaskan cara mengkonfigurasi alamat IP statis untuk Application Discovery Service Agentless Collector (Agentless Collector) VM. Saat pertama kali diinstal, kolektor VM dikonfigurasi untuk menggunakan Dynamic Host Configuration Protocol (DHCP).

> **Note**
>
> Kolektor Tanpa Agen mendukung. IPv4 Itu tidak mendukung IPv6.

Agentless Collector version 2

Untuk mengkonfigurasi alamat IP statis untuk kolektor VM

1. Kumpulkan informasi jaringan berikut dari VMware vCenter:

- Alamat IP statis — Alamat IP yang tidak ditandatangani di subnet. Misalnya, 192.168.1.138.
- CIDR netmask - Untuk mendapatkan netmask CIDR, periksa pengaturan alamat IP dari host vCenter yang menjadi tuan rumah VM VMware kolektor. Misalnya, /24.
- Default Gateway - Untuk mendapatkan gateway default, periksa pengaturan alamat IP dari host VMware vCenter yang menjadi tuan rumah VM kolektor. Misalnya, 192.168.1.1.
- DNS Primer — Untuk mendapatkan DNS primer, periksa pengaturan alamat IP dari host vCenter yang menghosting VMware VM kolektor. Misalnya, 192.168.1.1.
- (Opsional) DNS Sekunder
- (Opsional) Nama domain lokal - Ini memungkinkan kolektor untuk mencapai URL host vCenter tanpa nama domain.

2. Buka konsol VM kolektor dan masuk **`ec2-user`** menggunakan kata sandi **`collector`** seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

3. Nonaktifkan antarmuka jaringan, dengan memasukkan perintah berikut di terminal jarak jauh.

```
sudo ip link set ens192 down
```

4. Perbarui konfigurasi antarmuka dengan menggunakan langkah-langkah berikut.

   a. Buka 10- cloud-init-ens 192.network di editor vi dengan menggunakan perintah berikut.

   ```
   sudo vi /etc/systemd/network/10-cloud-init-ens192.network
   ```

   b. Perbarui nilai, seperti yang ditunjukkan pada contoh berikut, dengan informasi yang Anda kumpulkan di langkah Kumpulkan informasi jaringan.

   ```
   [Match]
   Name=ens192

   [Network]
   DHCP=no
   Address=static-ip-value/CIDR-netmask
   Gateway=gateway-value
   ```

```
DNS=dnsserver-value
```

5. Perbarui Domain Name System (DNS) menggunakan langkah-langkah berikut.

   a. Buka `resolv.conf` file di vi menggunakan perintah berikut.

   ```
   sudo vi /etc/resolv.conf
   ```

   b. Perbarui `resolv.conf` file di vi menggunakan perintah berikut.

   ```
   search localdomain-name
   options timeout:2 attempts:5
   nameserver dnsserver-value
   ```

   Contoh berikut menunjukkan `resolv.conf` file yang diedit.

   ```
   search vsphere.local
   options timeout:2 attempts:5
   nameserver 192.168.1.1
   ```

6. Aktifkan antarmuka jaringan, dengan memasukkan perintah berikut.

   ```
   sudo ip link set ens192 up
   ```

7. Reboot VM seperti yang ditunjukkan pada contoh berikut.

   ```
   sudo reboot
   ```

8. Verifikasi pengaturan jaringan Anda menggunakan langkah-langkah berikut.

   a. Periksa apakah alamat IP dikonfigurasi dengan benar, dengan memasukkan perintah berikut.

   ```
   ifconfig
   ip addr show
   ```

   b. Periksa apakah gateway ditambahkan dengan benar, dengan memasukkan perintah berikut.

   ```
   route -n
   ```

Outputnya harus mirip dengan contoh berikut.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
 Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0
 docker0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
```

c. Verifikasi bahwa Anda dapat melakukan ping ke URL publik, dengan memasukkan perintah berikut.

```
ping www.google.com
```

d. Verifikasi bahwa Anda dapat melakukan ping alamat IP vCenter atau nama host seperti yang ditunjukkan pada contoh berikut.

```
ping vcenter-host-url
```

Agentless Collector version 1

Untuk mengkonfigurasi alamat IP statis untuk kolektor VM

1. Kumpulkan informasi jaringan berikut dari VMware vCenter:

   - Alamat IP statis — Alamat IP yang tidak ditandatangani di subnet. Misalnya, 192.168.1.138.
   - Masker jaringan - Untuk mendapatkan mask jaringan, periksa pengaturan alamat IP dari host VMware vCenter yang menjadi tuan rumah VM kolektor. Misalnya, 255.255.255.0.
   - Default Gateway - Untuk mendapatkan gateway default, periksa pengaturan alamat IP dari host VMware vCenter yang menjadi tuan rumah VM kolektor. Misalnya, 192.168.1.1.
   - DNS Primer — Untuk mendapatkan DNS primer, periksa pengaturan alamat IP dari host vCenter yang menghosting VMware VM kolektor. Misalnya, 192.168.1.1.
   - (Opsional) DNS Sekunder
   - (Opsional) Nama domain lokal - Ini memungkinkan kolektor untuk mencapai URL host vCenter tanpa nama domain.

2. Buka konsol VM kolektor dan masuk **`ec2-user`** menggunakan kata sandi **`collector`** seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

3. Nonaktifkan antarmuka jaringan, dengan memasukkan perintah berikut di terminal jarak jauh.

```
sudo /sbin/ifdown eth0
```

4. Perbarui konfigurasi antarmuka eth0 menggunakan langkah-langkah berikut.

   a. Buka ifcfg-eth0 di editor vi menggunakan perintah berikut.

   ```
   sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

   b. Perbarui nilai antarmuka, seperti yang ditunjukkan pada contoh berikut, dengan informasi yang Anda kumpulkan di langkah Kumpulkan informasi jaringan.

   ```
   DEVICE=eth0
   BOOTPROTO=static
   ONBOOT=yes
   IPADDR=static-ip-value
   NETMASK=netmask-value
   GATEWAY=gateway-value
   TYPE=Ethernet
   USERCTL=yes
   PEERDNS=no
   RES_OPTIONS="timeout:2 attempts:5"
   ```

5. Perbarui Domain Name System (DNS) menggunakan langkah-langkah berikut.

   a. Buka `resolv.conf` file di vi menggunakan perintah berikut.

   ```
   sudo vi /etc/resolv.conf
   ```

   b. Perbarui `resolv.conf` file di vi menggunakan perintah berikut.

   ```
   search localdomain-name
   options timeout:2 attempts:5
   nameserver dnsserver-value
   ```

Contoh berikut menunjukkan `resolv.conf` file yang diedit.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Aktifkan antarmuka jaringan, dengan memasukkan perintah berikut.

```
sudo /sbin/ifup eth0
```

7. Reboot VM seperti yang ditunjukkan pada contoh berikut.

```
sudo reboot
```

8. Verifikasi pengaturan jaringan Anda menggunakan langkah-langkah berikut.

   a. Periksa apakah alamat IP dikonfigurasi dengan benar, dengan memasukkan perintah berikut.

   ```
   ifconfig
   ip addr show
   ```

   b. Periksa apakah gateway ditambahkan dengan benar, dengan memasukkan perintah berikut.

   ```
   route -n
   ```

   Outputnya harus mirip dengan contoh berikut.

   ```
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use
    Iface
   0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
   172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0
    docker0
   192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
   ```

   c. Verifikasi bahwa Anda dapat melakukan ping ke URL publik, dengan memasukkan perintah berikut.

```
ping www.google.com
```

d. Verifikasi bahwa Anda dapat melakukan ping alamat IP vCenter atau nama host seperti yang ditunjukkan pada contoh berikut.

```
ping vcenter-host-url
```

(Opsional) Setel ulang VM Kolektor Tanpa Agen kembali menggunakan DHCP

Langkah-langkah berikut menjelaskan cara mengkonfigurasi ulang VM Agentless Collector untuk menggunakan DHCP.

Agentless Collector version 2

Untuk mengkonfigurasi VM kolektor untuk menggunakan DHCP

1. Nonaktifkan antarmuka jaringan dengan menjalankan perintah berikut di terminal jarak jauh.

```
sudo ip link set ens192 down
```

2. Perbarui konfigurasi antarmuka dengan menggunakan langkah-langkah berikut.

   a. Buka `10-cloud-init-ens192.network` file di editor vi dengan menggunakan perintah berikut.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

   b. Perbarui nilai-nilai seperti yang ditunjukkan pada contoh berikut.

```
[Match]
Name=ens192

[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

3. Setel ulang pengaturan DNS, dengan memasukkan perintah berikut.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Aktifkan antarmuka jaringan, dengan memasukkan perintah berikut.

```
sudo ip link set ens192 up
```

5. Reboot kolektor VM seperti yang ditunjukkan pada contoh berikut.

```
sudo reboot
```

Agentless Collector version 1

Untuk mengkonfigurasi VM kolektor untuk menggunakan DHCP

1. Nonaktifkan antarmuka jaringan dengan menjalankan perintah berikut di terminal jarak jauh.

```
sudo /sbin/ifdown eth0
```

2. Perbarui konfigurasi jaringan dengan menggunakan langkah-langkah berikut.

   a. Buka `ifcfg-eth0` file di editor vi menggunakan perintah berikut.

   ```
   sudo /sbin/ifdown eth0
   ```

   b. Perbarui nilai-nilai dalam `ifcfg-eth0` file seperti yang ditunjukkan pada contoh berikut.

   ```
   DEVICE=eth0
   BOOTPROTO=dhcp
   ONBOOT=yes
   TYPE=Ethernet
   USERCTL=yes
   PEERDNS=yes
   DHCPV6C=yes
   DHCPV6C_OPTIONS=-nw
   PERSISTENT_DHCLIENT=yes
   RES_OPTIONS="timeout:2 attempts:5"
   ```

3. Setel ulang pengaturan DNS dengan memasukkan perintah berikut.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Aktifkan antarmuka jaringan dengan memasukkan perintah berikut.

```
sudo /sbin/ifup eth0
```

5. Reboot kolektor VM seperti yang ditunjukkan pada contoh berikut.

```
sudo reboot
```

(Opsional) Konfigurasikan protokol otentikasi Kerberos

Jika server OS Anda mendukung protokol otentikasi Kerberos, maka Anda dapat menggunakan protokol ini untuk terhubung ke server Anda. Untuk melakukannya, Anda harus mengkonfigurasi Application Discovery Service Agentless Collector VM.

Langkah-langkah berikut menjelaskan cara mengkonfigurasi protokol otentikasi Kerberos pada Application Discovery Service Agentless Collector VM Anda.

Untuk mengkonfigurasi protokol otentikasi Kerberos pada VM kolektor Anda

1. Buka konsol VM kolektor dan masuk **`ec2-user`** menggunakan kata sandi **`collector`** seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

2. Buka file `krb5.conf` konfigurasi di `/etc` folder. Untuk melakukannya, Anda dapat menggunakan contoh kode berikut.

```
cd /etc
sudo nano krb5.conf
```

3. Perbarui file `krb5.conf` konfigurasi dengan informasi berikut.

```
[libdefaults]
    forwardable = true
    dns_lookup_realm = true
    dns_lookup_kdc = true
```

```
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_realm = default_Kerberos_realm

[realms]
 default_Kerberos_realm = {
     kdc = KDC_hostname
     server_name = server_hostname
     default_domain = domain_to_expand_hostnames
 }

[domain_realm]
 .domain_name = default_Kerberos_realm
 domain_name = default_Kerberos_realm
```

Simpan file dan keluar dari editor teks.

4. Reboot kolektor VM seperti yang ditunjukkan pada contoh berikut.

```
sudo reboot
```

Menggunakan modul Pengumpulan Data Jaringan Kolektor Tanpa Agen

Modul Pengumpulan Data Jaringan memungkinkan Anda menemukan dependensi di antara server di pusat data lokal Anda. Data jaringan ini mempercepat perencanaan migrasi Anda dengan memberikan visibilitas tentang bagaimana aplikasi berkomunikasi di seluruh server.

Modul Pengumpulan Data Jaringan terhubung ke server yang diidentifikasi oleh modul VMware vCenter, dan menganalisis IP sumber ke IP/port lalu lintas tujuan untuk server tersebut.

Topik

- Menyiapkan modul Pengumpulan Data Jaringan
- Upaya pengumpulan data jaringan
- Status server dalam modul Pengumpulan Data Jaringan

Menyiapkan modul Pengumpulan Data Jaringan

Modul Pengumpulan Data Jaringan mengumpulkan data jaringan untuk inventaris server yang berasal dari modul VMware vCenter. Oleh karena itu, untuk menggunakan modul Network Data Collection, pertama mengatur modul VMware vCenter. Untuk instruksi, ikuti panduan dalam topik berikut:

1. the section called “Menyebarkan kolektor”
2. the section called “Mengakses konsol kolektor”
3. the section called “Mengkonfigurasi kolektor”
4. the section called “Menggunakan modul pengumpulan VMware data”

Untuk mengatur modul Pengumpulan Data Jaringan

1. Di dasbor Agentless Collector, di bagian Pengumpulan Data Jaringan, pilih Lihat koneksi jaringan.
2. Pada halaman Koneksi jaringan, pilih Edit kolektor.
3. Di bagian kredensial, masukkan setidaknya satu set kredensil. Anda dapat memasukkan hingga 10 set kredensil. Pertama kali modul mencoba mengumpulkan data untuk server, ia mencoba semua kredensional sampai menemukan satu set kredensional yang berfungsi; kemudian menyimpan set itu dan menggunakannya lagi dalam upaya berikutnya. Untuk informasi tentang menyiapkan kredensil, lihat. the section called “Menyiapkan kredensial”
4. Di bagian Preferensi pengumpulan data, untuk mulai mengumpulkan data secara otomatis saat server reboot, pilih Mulai pengumpulan data secara otomatis.
5. Jika Anda belum menyiapkan sertifikat WinRM, pilih Nonaktifkan pemeriksaan sertifikat WinRM.
6. Pilih Simpan.
7. Pengumpulan terjadi di server setiap 15 detik. Untuk melihat detail upaya pengumpulan untuk server tertentu, pilih kotak centang di sebelah kiri server dalam tabel Server.

Menyiapkan kredensial

Modul Pengumpulan Data Jaringan menggunakan WinRM untuk mengumpulkan data dari server Windows. Ini menggunakan SNMPv2 dan SNMPv3 mengumpulkan data dari server Linux.

Kredensi WinRM:

- Tentukan nama pengguna dan kata sandi akun Windows yang memiliki yang berikut:
  - Baca akses ke `\root\standardcimv2` namespace
  - Baca izin untuk kelas `MSFT_NetTCPConnection`
  - Akses WMI jarak jauh
- Kami menyarankan Anda membuat akun layanan khusus dengan izin minimal yang diperlukan.
- Hindari menggunakan administrator domain atau akun administrator lokal.
- Port 5986 (HTTPS) harus terbuka antara kolektor dan server target.
- Hindari menonaktifkan pemeriksaan sertifikat WinRM. Untuk informasi tentang menyiapkan sertifikat WinRM, lihat. the section called “Mengatasi masalah sertifikasi yang ditandatangani sendiri saat mengonfigurasi sertifikat WinRM”

SNMPv2 kredensi:

- Berikan string komunitas read-only yang dapat mengakses 1.3.6.1.2.1.6.13.* OID
- SNMPv3 lebih disukai SNMPv2 karena peningkatan keamanan di SNMPv3
- Port 161/UDP harus terbuka antara kolektor dan server target
- Gunakan string komunitas non-default yang kompleks
- Hindari string umum seperti “publik” atau “pribadi”
- Perlakukan string komunitas seperti kata sandi

SNMPv3 credentials

- Berikan username/password dan auth/privacy detail dengan izin hanya-baca yang dapat mengakses 1.3.6.1.2.1.6.13.* OID.
- Port 161/UDP harus terbuka antara kolektor dan server target
- Aktifkan otentikasi dan privasi
- Gunakan protokol otentikasi yang kuat (SHA lebih disukai daripada) MD5
- Gunakan protokol enkripsi yang kuat (AES lebih disukai daripada DES)
- Gunakan kata sandi yang kompleks untuk autentikasi dan privasi
- Gunakan nama pengguna unik (hindari nama umum)

Praktik terbaik umum untuk Manajemen Kredensi

- Simpan kredensil dengan aman
- Putar semua kredensil secara teratur
- Gunakan pengelola kata sandi atau brankas aman
- Pantau penggunaan kredensi
- Ikuti prinsip hak istimewa terkecil dan hanya berikan izin minimum yang diperlukan

Upaya pengumpulan data jaringan

Ketika server baru ditemukan, kolektor mencoba setiap kredensi yang dikonfigurasi untuk setiap alamat IP. Setelah kolektor menemukan kredensi yang valid, ia hanya menggunakan kredensi itu. Setelah dua kegagalan berturut-turut, kolektor mencoba mengumpulkan data jaringan untuk server setelah 30 menit, 2 jam, 8 jam, dan kemudian 24 jam. Setelah 6 upaya gagal, kolektor terus mencoba semua kredensi yang dikonfigurasi sekali setiap hari. Untuk mengatasi masalah ini, edit kredensial saat ini atau tambahkan yang tambahan dengan memilih Edit kolektor, atau buat perubahan pada server target yang sedang dipantau.

Status server dalam modul Pengumpulan Data Jaringan

Tabel berikut menjelaskan nilai status koleksi.

Status	Arti
Mengumpulkan atau Mengumpulkan	Upaya pengumpulan terakhir untuk koneksi jaringan berhasil.
Kesalahan atau Kesalahan	Upaya pengumpulan terakhir untuk koneksi jaringan gagal karena masalah jaringan atau izin. Untuk informasi tambahan, pilih kotak centang di sebelah kiri server yang memiliki kesalahan.
Dilewati	Server yang tidak memiliki kredensialnya valid. Perbarui atau konfigurasikan kredenal server tambahan.

Status	Arti
Tidak ada data	Pengumpulan data untuk server belum dimulai. Untuk mulai mengumpulkan data, pilih Mulai kolektor.
Tertunda	Pengumpulan telah dimulai tetapi tidak ada upaya pengumpulan yang dilakukan. Tunggu beberapa menit, lalu segarkan daftarnya.

Menggunakan modul pengumpulan VMware data vCenter Agentless Collector

Bagian ini menjelaskan modul pengumpulan data VMware vCenter Application Discovery Service Agentless Collector (Agentless Collector), yang digunakan untuk mengumpulkan inventaris server, profil, dan data pemanfaatan dari Anda. VMware VMs

Topik

- Menyiapkan modul pengumpulan data Agentless Collector untuk vCenter VMware
- Melihat detail pengumpulan VMware data
- Mengontrol ruang lingkup pengumpulan data vCenter
- Data yang dikumpulkan oleh modul pengumpulan data VMware vCenter Kolektor Tanpa Agen

Menyiapkan modul pengumpulan data Agentless Collector untuk vCenter VMware

Bagian ini menjelaskan cara mengatur modul pengumpulan data VMware vCenter Kolektor Tanpa Agen untuk mengumpulkan inventaris server, profil, dan data pemanfaatan dari Anda. VMware VMs

> **Note**
>
> Sebelum memulai penyiapan vCenter, pastikan Anda dapat memberikan kredensi vCenter dengan izin Baca dan Lihat yang ditetapkan untuk grup Sistem.

Untuk mengatur modul pengumpulan data VMware vCenter

1. Pada halaman dasbor Agentless Collector, di bawah Pengumpulan data, pilih Mengatur di bagian vCenterVMware .
2. Pada halaman Mengatur pengumpulan data VMware vCenter, lakukan hal berikut:

   a. Di bawah kredensi vCenter:

      i. Untuk URL/IP vCenter, masukkan alamat IP host Server VMware vCenter Anda.

      ii. Untuk Nama Pengguna vCenter, masukkan nama pengguna lokal atau domain yang digunakan kolektor untuk berkomunikasi dengan vCenter. Untuk pengguna domain, gunakan formulir domain\nama pengguna atau nama pengguna@domain.

      iii. Untuk Kata Sandi vCenter, masukkan kata sandi pengguna lokal atau domain.

   b. Di bawah Preferensi pengumpulan data:

      • Untuk mulai mengumpulkan data secara otomatis segera setelah penyiapan yang berhasil, pilih Mulai pengumpulan data secara otomatis.

   c. Pilih Siapkan.

Selanjutnya, Anda akan melihat halaman detail pengumpulan VMware data, yang dijelaskan dalam topik berikutnya.

Melihat detail pengumpulan VMware data

Halaman detail pengumpulan VMware data menunjukkan detail tentang vCenter tempat Anda mengatur. Menyiapkan modul pengumpulan data Agentless Collector untuk vCenter VMware

Di bawah server vCenter Ditemukan, vCenter yang Anda atur terdaftar dengan informasi berikut tentang vCenter:

- Alamat IP dari server vCenter.
- Jumlah server di vCenter.
- Status pengumpulan data.
- Berapa lama sejak pembaruan terakhir.

Pilih Hapus server vCenter untuk menghapus server vCenter yang ditampilkan dan mengembalikan Anda ke halaman Mengatur pengumpulan data vCenter VMware .

Jika Anda tidak memilih untuk memulai pengumpulan data secara otomatis, Anda dapat memulai pengumpulan data dengan menggunakan tombol Mulai pengumpulan data di halaman ini. Setelah pengumpulan data dimulai, tombol mulai berubah menjadi Hentikan pengumpulan data.

Jika kolom Status koleksi menunjukkan Mengumpulkan, pengumpulan data telah dimulai.

Anda melihat data yang dikumpulkan di AWS Migration Hub konsol. Jika Anda mengumpulkan data untuk inventaris server VMware vCenter, Anda dapat mengakses data yang muncul di konsol sekitar 15 menit setelah mengaktifkan pengumpulan data.

Anda dapat memilih Lihat server di Migration Hub di halaman ini untuk membuka konsol Migration Hub, jika akses Anda ke internet tidak diblokir. Apakah Anda memilih tombol ini atau tidak, untuk informasi tentang cara mengakses konsol Hub Migrasi, lihatMelihat data yang Anda kumpulkan.

Berikut ini adalah pedoman panjang pengumpulan data yang direkomendasikan sesuai dengan kegiatan perencanaan migrasi:

- TCO (total biaya kepemilikan) - 2 hingga 4 minggu
- Perencanaan migrasi - 2 hingga 6 minggu

Mengontrol ruang lingkup pengumpulan data vCenter

Pengguna vCenter memerlukan izin baca-saja pada setiap host ESX atau VM untuk inventaris menggunakan Application Discovery Service. Menggunakan pengaturan izin, Anda dapat mengontrol host VMs mana dan termasuk dalam pengumpulan data. Anda dapat mengizinkan semua host dan VMs di bawah vCenter saat ini untuk diinventarisasi, atau memberikan izin berdasarkan. case-by-case

> **Note**
>
> Sebagai praktik keamanan terbaik, kami menyarankan agar tidak memberikan izin tambahan yang tidak diperlukan kepada pengguna vCenter dari Application Discovery Service.

Prosedur berikut menjelaskan skenario konfigurasi yang diurutkan dari yang paling tidak terperinci hingga yang paling terperinci. Prosedur ini untuk VSphere Client v6.7.0.2. Prosedur untuk versi lain dari klien mungkin berbeda, tergantung pada versi klien vSphere yang Anda gunakan.

Untuk menemukan data tentang semua host ESX dan VMs di bawah vCenter saat ini

1. Di klien VMware vSphere Anda, pilih vCenter dan kemudian pilih Host dan Cluster atau dan Template. VMs
2. Pilih sumber daya pusat data dan kemudian pilih Izin.
3. Pilih pengguna vCenter dan kemudian pilih simbol untuk menambah, mengedit, atau menghapus peran pengguna.
4. Pilih Read-only dari menu Peran.
5. Pilih Propagate to children lalu pilih OK.

Untuk menemukan data tentang host ESX tertentu dan semua objek anaknya

1. Di klien VMware vSphere Anda, pilih vCenter dan kemudian pilih Host dan Cluster atau dan Template. VMs
2. Pilih Objek Terkait, Host.
3. Buka menu konteks (klik kanan) untuk nama host dan pilih Semua Tindakan vCenter, Tambah Izin.
4. Di bawah Tambah Izin, tambahkan pengguna vCenter ke host. Untuk Peran yang Ditetapkan, pilih Hanya Baca.
5. Pilih Sebarkan ke anak-anak, OK.

Untuk menemukan data tentang host ESX tertentu atau VM anak

1. Di klien VMware vSphere Anda, pilih vCenter dan kemudian pilih Host dan Cluster atau dan Template. VMs
2. Pilih Objek Terkait.
3. Pilih Host (menampilkan daftar host ESX yang dikenal vCenter) atau Mesin Virtual (menampilkan daftar VMs di semua host ESX).
4. Buka menu konteks (klik kanan) untuk nama host atau VM dan pilih Semua Tindakan vCenter, Tambah Izin.
5. Di bawah Tambah Izin, tambahkan pengguna vCenter ke host atau VM. Untuk Peran yang Ditetapkan, pilih Hanya Baca.
6. Pilih OK.

> **Note**
>
> Jika Anda memilih Propagate to children, Anda masih dapat menghapus izin hanya-baca dari host ESX dan VMs atas dasar. case-by-case Opsi ini tidak berpengaruh pada izin yang diwariskan yang berlaku untuk host ESX lainnya dan. VMs

Data yang dikumpulkan oleh modul pengumpulan data VMware vCenter Kolektor Tanpa Agen

Informasi berikut menjelaskan data yang dikumpulkan oleh modul pengumpulan data vCenter VMware Application Discovery Service Agentless Collector (Agentless Collector). Untuk informasi tentang pengaturan pengumpulan data, lihatMenyiapkan modul pengumpulan data Agentless Collector untuk vCenter VMware.

Legenda tabel untuk Agentless Collector VMware vCenter mengumpulkan data:

- Data yang dikumpulkan adalah dalam pengukuran kilobyte (KB) kecuali dinyatakan lain.
- Data setara di konsol Migration Hub dilaporkan dalam megabyte (MB).
- Bidang data yang dilambangkan dengan tanda bintang (*) hanya tersedia dalam file.csv yang dihasilkan dari fungsi ekspor Application Discovery Service API.

  Agentless Collector mendukung ekspor data menggunakan CLI AWS . Untuk mengekspor data yang dikumpulkan menggunakan AWS CLI, ikuti petunjuk yang dijelaskan di bawah Ekspor Data Kinerja Sistem untuk Semua Server pada halaman Ekspor Data yang Dikumpulkan dalam Panduan Pengguna Application Discovery Service.
- Periode polling berada dalam interval sekitar 60 menit.
- Bidang data dilambangkan dengan tanda bintang ganda (**) saat ini mengembalikan nilai nol.

Bidang data	Deskripsi
applicationConfigurationId*	ID aplikasi migrasi VM dikelompokkan di bawah.
avgCpuUsagePct	Persentase rata-rata penggunaan CPU selama periode polling.

Bidang data	Deskripsi
avgDiskBytesReadPerSecond	Jumlah rata-rata byte yang dibaca dari disk selama periode polling.
avgDiskBytesWrittenPerSecond	Jumlah rata-rata byte yang ditulis ke disk selama periode polling.
avgDiskReadOpsPerSecond**	Jumlah rata-rata I/O operasi baca per detik nol.
avgDiskWriteOpsPerSecond**	Rata-rata jumlah I/O operasi tulis per detik.
avgFreeRAM	RAM gratis rata-rata dinyatakan dalam MB.
avgNetworkBytesReadPerSecond	Jumlah rata-rata throughput byte yang dibaca per detik.
avgNetworkBytesWrittenPerSecond	Jumlah rata-rata throughput byte yang ditulis per detik.
ComputerManufacturer	Vendor dilaporkan oleh ESXi tuan rumah.
ComputerModel	Model komputer dilaporkan oleh ESXi tuan rumah.
configId	ID yang ditetapkan oleh Application Discovery Service ke VM yang ditemukan.
configType	Jenis sumber daya yang ditemukan.
connectorId	ID alat virtual.
cpuType	vCPU untuk VM, model aktual untuk host.
datacenterId	ID dari vCenter.
hostId*	ID host VM.
hostName	Nama host yang menjalankan perangkat lunak virtualisasi.

Bidang data	Deskripsi
hypervisor	Jenis hypervisor.
id	ID server.
lastModifiedTime Stempel *	Tanggal dan waktu pengumpulan data terbaru sebelum ekspor data.
macAddress	Alamat MAC dari VM.
manufacturer	Pembuat perangkat lunak virtualisasi.
maxCpuUsagePct	Maks. persentase penggunaan CPU selama periode polling.
maxDiskBytesReadPerSecond	Maks. jumlah byte yang dibaca dari disk selama periode polling.
maxDiskBytesWrittenPerSecond	Maks. jumlah byte yang ditulis ke disk selama periode polling.
maxDiskReadOpsPerSecond **	Maks. jumlah I/O operasi baca per detik.
maxDiskWriteOpsPerSecond **	Maks. jumlah I/O operasi tulis per detik.
maxNetworkBytesReadPerSecond	Maks. jumlah throughput byte yang dibaca per detik.
maxNetworkBytesWrittenPerSecond	Maks. jumlah throughput byte yang ditulis per detik.
MemoryReservation *	Batasi untuk menghindari komitmen memori yang berlebihan pada VM.
moRefId	ID Referensi Objek Dikelola vCenter Unik.
nama*	Nama VM atau jaringan (ditentukan pengguna).
numCores	Jumlah core CPU yang ditetapkan untuk VM.

Bidang data	Deskripsi
numCpus	Jumlah soket CPU pada ESXi host.
numDisks**	Jumlah disk pada VM.
numNetworkCards**	Jumlah kartu jaringan pada VM.
osName	Nama sistem operasi pada VM.
osVersion	Versi sistem operasi pada VM.
portGroupId*	ID grup port anggota VLAN.
portGroupName*	Nama grup port anggota VLAN.
powerState*	Status kekuasaan.
serverId	Application Discovery Service menetapkan ID ke VM yang ditemukan.
smBiosId*	ID/versi BIOS manajemen sistem.
negara bagian*	Status alat virtual.
toolsStatus	Keadaan VMware alat operasional
totalDiskFreeUkuran	Ruang disk kosong dinyatakan dalam MB. Tersedia untuk vCenter Server 7.0 dan versi yang lebih baru.
totalDiskSize	Total kapasitas disk yang dinyatakan dalam MB.
totalRAM	Jumlah total RAM yang tersedia di VM dalam MB.
jenis	Jenis host.
vCenterId	Nomor ID unik dari VM.

Bidang data	Deskripsi
vCenterName*	Nama host vCenter.
virtualSwitchName*	Nama sakelar virtual.
vmFolderPath	Jalur direktori file VM.
vmName	Nama mesin virtual.

Menggunakan modul pengumpulan data database dan analitik

Bagian ini menjelaskan cara mengatur, mengonfigurasi, dan menggunakan modul pengumpulan data database dan analitik. Anda dapat menggunakan modul pengumpulan data ini untuk terhubung ke lingkungan data Anda dan mengumpulkan metadata dan metrik kinerja dari database lokal dan server analitik. Untuk informasi tentang metrik yang dapat Anda kumpulkan dengan modul ini, lihatData yang dikumpulkan oleh database Agentless Collector dan modul pengumpulan data analitik.

> **Important**
>
> Pemberitahuan akhir dukungan: Pada 20 Mei 2026, AWS akan mengakhiri dukungan untuk Penasihat AWS Database Migration Service Armada. Setelah 20 Mei 2026, Anda tidak akan lagi dapat mengakses konsol Penasihat AWS DMS Armada atau sumber daya Penasihat AWS DMS Armada. Untuk informasi lebih lanjut, lihat akhir dukungan AWS DMS Fleet Advisor.

Pada tingkat tinggi, saat menggunakan modul pengumpulan data database dan analitik, Anda mengambil langkah-langkah berikut.

1. Selesaikan langkah-langkah prasyarat, konfigurasikan pengguna IAM Anda, dan buat pengumpul data. AWS DMS
2. Konfigurasikan penerusan data untuk memastikan bahwa modul pengumpulan data Anda dapat mengirim metadata yang dikumpulkan dan metrik kinerja ke. AWS
3. Tambahkan server LDAP Anda dan gunakan untuk menemukan server OS di lingkungan data Anda. Atau, tambahkan server OS Anda secara manual atau gunakan fileMenggunakan modul pengumpulan VMware data.

4. Konfigurasikan kredenal koneksi ke server OS Anda dan kemudian gunakan untuk menemukan server database.
5. Konfigurasikan kredenal koneksi ke database dan server analitik Anda, lalu jalankan pengumpulan data. Untuk informasi selengkapnya, lihat Pengumpulan data database dan analitik.
6. Lihat data yang dikumpulkan di AWS DMS konsol dan gunakan untuk menghasilkan rekomendasi target untuk migrasi ke konsol AWS Cloud. Untuk informasi selengkapnya, lihat Pengumpulan data database dan analitik.

Topik

- Server OS, database, dan analitik yang didukung
- Membuat pengumpul AWS DMS data
- Mengkonfigurasi penerusan data
- Menambahkan server LDAP dan OS
- Menemukan server database Anda
- Data yang dikumpulkan oleh database Agentless Collector dan modul pengumpulan data analitik

Server OS, database, dan analitik yang didukung

Modul pengumpulan data database dan analitik di Agentless Collector mendukung server Microsoft Active Directory LDAP.

Modul pengumpulan data ini mendukung server OS berikut.

- Amazon Linux 2
- CentOS Linux versi 6 dan lebih tinggi
- Debian versi 10 dan lebih tinggi
- Red Hat Enterprise Linux versi 7 dan lebih tinggi
- SUSE Linux Enterprise Server versi 12 dan lebih tinggi
- Ubuntu versi 16.01 dan lebih tinggi
- Windows Server 2012 dan lebih tinggi
- Windows XP dan lebih tinggi

Selain itu, modul pengumpulan data database dan analitik mendukung server database berikut.

- Microsoft SQL Server versi 2012 dan hingga 2019
- MySQL versi 5.6 dan hingga 8
- Oracle versi 11g Rilis 2 dan hingga 12c, 19c, dan 21c
- PostgreSQL versi 9.6 dan hingga 13

Membuat pengumpul AWS DMS data

Modul pengumpulan data database dan analitik Anda menggunakan pengumpul AWS DMS data untuk berinteraksi dengan AWS DMS konsol. Anda dapat melihat data yang dikumpulkan di AWS DMS konsol, atau menggunakannya untuk menentukan mesin AWS target berukuran tepat. Untuk informasi selengkapnya, lihat Menggunakan fitur Rekomendasi Target Penasihat AWS DMS Armada.

Sebelum membuat pengumpul AWS DMS data, buat peran IAM yang digunakan pengumpul AWS DMS data untuk mengakses bucket Amazon S3. Anda membuat bucket Amazon S3 ini saat Anda menyelesaikan prasyarat di. Prasyarat untuk Kolektor Tanpa Agen

Untuk membuat peran IAM bagi pengumpul AWS DMS data Anda untuk mengakses Amazon S3

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran, lalu pilih Buat peran.
3. Pada halaman Pilih entitas tepercaya, untuk jenis entitas tepercaya, pilih AWS Layanan. Untuk kasus penggunaan untuk AWS layanan lain, pilih DMS.
4. Pilih kotak centang DMS dan pilih Berikutnya.
5. Pada halaman Tambahkan izin, pilih FleetAdvisorS3Policy yang Anda buat sebelumnya. Pilih Berikutnya.
6. Pada halaman Nama, tinjau, dan buat, masukkan **`FleetAdvisorS3Role`** nama Peran, lalu pilih Buat peran.
7. Buka peran yang Anda buat, dan pilih tab Trust relationship. Pilih Edit kebijakan kepercayaan.
8. Pada halaman Edit kebijakan kepercayaan, tempelkan JSON berikut ke editor, ganti kode yang ada.

   JSON

```
{
```

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

9. Pilih Perbarui kebijakan.

Sekarang, buat pengumpul data di AWS DMS konsol.

Untuk membuat pengumpul AWS DMS data

1. Masuk ke Konsol Manajemen AWS dan buka AWS DMS konsol di https://console.aws.amazon.com/dms/v2/.
2. Pilih Wilayah AWS yang Anda tetapkan sebagai Wilayah beranda Hub Migrasi. Untuk informasi selengkapnya, lihat Masuk ke Migration Hub dan pilih Wilayah beranda.
3. Di panel navigasi, pilih Pengumpul data di bawah Temukan. Halaman pengumpul data terbuka.
4. Pilih Buat pengumpul data. Halaman Buat pengumpul data terbuka.
5. Untuk Nama di bagian Konfigurasi umum, masukkan nama pengumpul data Anda.
6. Di bagian Konektivitas, pilih Browse S3. Pilih bucket Amazon S3 yang Anda buat sebelumnya dari daftar.
7. Untuk peran IAM, pilih `FleetAdvisorS3Role` yang Anda buat sebelumnya.
8. Pilih Buat pengumpul data.

Mengkonfigurasi penerusan data

Setelah Anda membuat AWS sumber daya yang diperlukan, konfigurasikan penerusan data dari database dan modul pengumpulan data analitik ke kolektor Anda AWS DMS .

Untuk mengkonfigurasi penerusan data

1. Buka konsol Agentless Collector. Untuk informasi selengkapnya, lihat Mengakses konsol kolektor.
2. Pilih Lihat Database dan kolektor analitik.
3. Pada halaman Dasbor, pilih Konfigurasi penerusan data di bagian Penerusan data.
4. Untuk Wilayah AWSID kunci akses IAM, dan kunci akses rahasia IAM, Agentless Collector Anda menggunakan nilai yang Anda konfigurasikan sebelumnya. Untuk informasi selengkapnya, lihat Masuk ke Migration Hub dan pilih Wilayah beranda dan Menyebarkan kolektor.
5. Untuk pengumpul data DMS Terhubung, pilih pengumpul data yang Anda buat di AWS DMS konsol.
6. Pilih Simpan.

Setelah Anda mengonfigurasi penerusan data, periksa bagian Penerusan data di halaman Dasbor. Pastikan modul pengumpulan data database dan analitik Anda menampilkan Connected for Access to DMS dan Access to S3.

Menambahkan server LDAP dan OS

Modul pengumpulan data database dan analitik menggunakan LDAP di Microsoft Active Directory untuk mengumpulkan informasi tentang OS, database, dan server analitik di jaringan Anda. Lightweight Directory Access Protocol (LDAP) adalah protokol aplikasi standar terbuka. Anda dapat menggunakan protokol ini untuk mengakses dan memelihara layanan informasi direktori terdistribusi melalui jaringan IP Anda.

Anda dapat menambahkan server LDAP yang ada ke dalam database dan modul pengumpulan data analitik Anda untuk secara otomatis menemukan server OS di jaringan Anda. Jika Anda tidak menggunakan LDAP, Anda dapat menambahkan server OS secara manual.

Untuk menambahkan server LDAP ke database dan modul pengumpulan data analitik Anda

1. Buka konsol Agentless Collector. Untuk informasi selengkapnya, lihat Mengakses konsol kolektor.
2. Pilih Lihat Database dan kolektor analitik, lalu pilih server LDAP di bawah Discovery di panel navigasi.
3. Pilih Tambahkan server LDAP. Halaman Add LDAP server terbuka.

4. Untuk Hostname, masukkan nama host server LDAP Anda.
5. Untuk Port, masukkan nomor port yang digunakan untuk permintaan LDAP.
6. Untuk nama Pengguna, masukkan nama pengguna yang Anda gunakan untuk terhubung ke server LDAP Anda.
7. Untuk Kata Sandi, masukkan kata sandi yang Anda gunakan untuk terhubung ke server LDAP Anda.
8. (Opsional) Pilih Verifikasi koneksi untuk memastikan bahwa Anda menambahkan kredensi server LDAP Anda dengan benar. Atau, Anda dapat memverifikasi kredenal koneksi server LDAP Anda nanti, dari daftar di halaman server LDAP.
9. Pilih Tambahkan server LDAP.
10. Pada halaman server LDAP, pilih server LDAP Anda dari daftar dan pilih Discover OS server.

> **Important**
>
> Untuk penemuan OS, modul pengumpulan data memerlukan kredensil untuk server domain untuk menjalankan permintaan menggunakan protokol LDAP.

Modul pengumpulan data database dan analitik terhubung ke server LDAP Anda dan menemukan server OS Anda. Setelah modul pengumpulan data menyelesaikan penemuan server OS, Anda dapat melihat daftar server OS yang ditemukan dengan memilih View OS server.

Atau, Anda dapat menambahkan server OS Anda secara manual atau mengimpor daftar server dari file nilai yang dipisahkan koma (CSV). Selain itu, Anda dapat menggunakan modul pengumpulan data VMware vCenter Agentless Collector untuk menemukan server OS Anda. Untuk informasi selengkapnya, lihat Menggunakan modul pengumpulan VMware data.

Untuk menambahkan server OS ke database dan modul pengumpulan data analitik

1. Pada halaman Database dan kolektor analitik, pilih server OS di bawah Discovery di panel navigasi.
2. Pilih Tambahkan server OS. Halaman Add OS server terbuka.
3. Berikan kredensil server OS Anda.

    a. Untuk jenis OS, pilih sistem operasi server Anda.

    b. Untuk Hostname/IP, masukkan nama host atau alamat IP server OS Anda.

c. Untuk Port, masukkan nomor port yang digunakan untuk kueri jarak jauh.

d. Untuk jenis otentikasi, pilih jenis otentikasi yang digunakan server OS Anda.

e. Untuk nama Pengguna, masukkan nama pengguna yang Anda gunakan untuk terhubung ke server OS Anda.

f. Untuk Kata Sandi, masukkan kata sandi yang Anda gunakan untuk terhubung ke server OS Anda.

g. Pilih Verifikasi untuk memastikan bahwa Anda menambahkan kredensi server OS Anda dengan benar.

4. (Opsional) Tambahkan beberapa server OS dari file CSV.

a. Pilih Server OS impor massal dari CSV.

b. Pilih Unduh templat untuk menyimpan file CSV yang menyertakan templat yang dapat Anda sesuaikan.

c. Masukkan kredensi koneksi untuk server OS Anda ke dalam file sesuai dengan template. Contoh berikut menunjukkan bagaimana Anda dapat memberikan kredensi koneksi server OS dalam file CSV.

```
OS type,Hostname/IP,Port,Authentication type,Username,Password
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

Simpan file CSV Anda setelah Anda menambahkan kredensi untuk semua server OS Anda.

d. Pilih Browse, lalu pilih file CSV Anda.

5. Pilih Tambahkan server OS.

6. Setelah Anda menambahkan kredensi untuk semua server OS, pilih server OS Anda dan pilih Temukan server database.

Menemukan server database Anda

Bagian ini memandu Anda melalui langkah-langkah yang harus Anda ambil untuk mengonfigurasi sistem operasi dan server basis data Anda. Kemudian, Anda akan menemukan server Anda dan memiliki opsi untuk menambahkan database atau server analitik secara manual.

Untuk penemuan database, Anda harus membuat pengguna untuk database sumber Anda dengan izin minimum yang diperlukan untuk modul pengumpulan data. Untuk informasi selengkapnya,

lihat Membuat pengguna database untuk Penasihat AWS DMS Armada di Panduan AWS DMS Pengguna.

Mengkonfigurasi pengaturan

Untuk menemukan database yang berjalan pada Server OS yang ditambahkan sebelumnya, modul pengumpulan data memerlukan akses ke sistem operasi dan server database. Halaman ini menguraikan langkah-langkah yang perlu Anda ambil untuk memastikan bahwa database Anda dapat diakses di port yang Anda tentukan dalam pengaturan koneksi. Anda juga akan mengaktifkan otentikasi jarak jauh di server database Anda dan memberikan modul pengumpulan data Anda dengan izin.

Konfigurasikan pengaturan di Linux

Selesaikan prosedur berikut untuk mengkonfigurasi pengaturan untuk menemukan server database di Linux.

Untuk mengkonfigurasi Linux untuk menemukan server database

1. Berikan akses sudo ke `netstat` perintah `ss` dan.

   Contoh kode berikut memberikan akses sudo ke perintah `ss` dan`netstat`.

   ```
   sudo bash -c "cat << EOF >> /etc/sudoers.d/username
   username ALL=(ALL) NOPASSWD: /usr/bin/ss
   username ALL=(ALL) NOPASSWD: /usr/bin/netstat
   EOF"
   ```

   Pada contoh sebelumnya, ganti *`username`* dengan nama pengguna Linux yang Anda tentukan dalam kredenal koneksi server OS.

   Contoh sebelumnya menggunakan `/usr/bin/` path to the `ss` and `netstat` command. Jalur ini mungkin berbeda di lingkungan Anda. Untuk menentukan jalur ke `netstat` perintah `ss` dan, jalankan `which netstat` perintah `which ss` dan.
2. Konfigurasikan server Linux Anda untuk memungkinkan menjalankan skrip SSH jarak jauh dan memungkinkan lalu lintas Internet Control Message Protocol (ICMP).

Konfigurasikan pengaturan di Microsoft Windows

Selesaikan prosedur berikut untuk mengonfigurasi pengaturan untuk menemukan server database di Microsoft Windows.

Untuk mengkonfigurasi Microsoft Windows untuk menemukan server database

1. Berikan kredensil dengan hibah untuk menjalankan kueri Windows Management Instrumentation (WMI) dan WMI Query Language (WQL) dan baca registri.
2. Tambahkan pengguna Windows yang Anda tentukan dalam kredenal koneksi server OS ke grup berikut: Pengguna COM Terdistribusi, Pengguna Log Kinerja, Pengguna Monitor Kinerja, dan Pembaca Log Peristiwa. Untuk melakukannya, gunakan contoh kode berikut.

   ```
   net localgroup "Distributed COM Users" username /ADD
   net localgroup "Performance Log Users" username /ADD
   net localgroup "Performance Monitor Users" username /ADD
   net localgroup "Event Log Readers" username /ADD
   ```

   Pada contoh sebelumnya, ganti *username* dengan nama pengguna Windows yang Anda tentukan dalam kredenal koneksi server OS.
3. Berikan izin yang diperlukan untuk pengguna Windows yang Anda tentukan dalam kredenial koneksi server OS.

   - Untuk Properti Manajemen dan Instrumentasi Windows, pilih Peluncuran Lokal dan Aktivasi Jarak Jauh.
   - Untuk Kontrol WMI, pilih izin Execute Methods, Enable Account, Remote Enable, dan Read Security untuk`CIMV2`, `DEFAULTStandartCimv2`, dan `WMI` ruang nama.
   - Untuk plug-in WMI, jalankan **`winrm configsddl default`** dan kemudian pilih Baca dan Jalankan.
4. Konfigurasikan host Windows Anda dengan menggunakan contoh kode berikut.

   ```
   netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
    dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
   netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
    dir=in action=allow # Allows ICPM traffic

   Enable-PSRemoting -Force # Enables WinRM
   Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
    startup
   ```

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
 specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '@{Negotiation="true"}' # Allow Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

Menemukan server database

Selesaikan serangkaian tugas berikut untuk menemukan dan menambahkan server database di konsol.

Untuk memulai penemuan server database Anda

1. Pada halaman Database dan kolektor analitik, pilih server OS di bawah Discovery di panel navigasi.
2. Pilih server OS yang menyertakan server database dan analitik Anda, lalu pilih Verifikasi koneksi pada menu Tindakan.
3. Untuk server yang memiliki status Konektivitas Gagal, edit kredenal koneksi.
    a. Pilih satu server atau beberapa server ketika mereka memiliki kredensialnya yang identik, lalu pilih Edit pada menu Tindakan. Halaman server Edit OS terbuka.
    b. Untuk Port, masukkan nomor port yang digunakan untuk kueri jarak jauh.
    c. Untuk jenis otentikasi, pilih jenis otentikasi yang digunakan server OS Anda.
    d. Untuk nama Pengguna, masukkan nama pengguna yang Anda gunakan untuk terhubung ke server OS Anda.
    e. Untuk Kata Sandi, masukkan kata sandi yang Anda gunakan untuk terhubung ke server OS Anda.
    f. Pilih Verifikasi koneksi untuk memastikan bahwa Anda memperbarui kredensi server OS Anda dengan benar. Selanjutnya, pilih Simpan.
4. Setelah memperbarui kredensi untuk semua server OS, pilih server OS Anda dan pilih Discover database server.

Modul pengumpulan data database dan analitik terhubung ke server OS Anda dan menemukan database dan server analitik yang didukung. Setelah modul pengumpulan data menyelesaikan

penemuan, Anda dapat melihat daftar database yang ditemukan dan server analitik dengan memilih Lihat server database.

Atau, Anda dapat menambahkan database dan server analitik Anda ke inventaris secara manual. Selain itu, Anda dapat mengimpor daftar server dari file CSV. Anda dapat melewati langkah ini jika Anda sudah menambahkan semua database dan server analitik Anda ke inventaris.

Untuk menambahkan database atau server analitik secara manual

1. Pada halaman Database dan pengumpul analitik, pilih Pengumpulan data di panel navigasi.
2. Pilih Tambahkan server basis data. Halaman Add database server terbuka.
3. Berikan kredensi server database Anda.

    a. Untuk mesin Database, pilih mesin database server Anda. Untuk informasi selengkapnya, lihat Server OS, database, dan analitik yang didukung.

    b. Untuk Hostname /IP, masukkan nama host atau alamat IP database atau server analitik Anda.

    c. Untuk Port, masukkan port tempat server Anda berjalan.

    d. Untuk jenis otentikasi, pilih jenis otentikasi yang digunakan database atau server analitik Anda.

    e. Untuk nama Pengguna, masukkan nama pengguna yang Anda gunakan untuk terhubung ke server Anda.

    f. Untuk Kata Sandi, masukkan kata sandi yang Anda gunakan untuk terhubung ke server Anda.

    g. Pilih Verifikasi untuk memastikan bahwa Anda menambahkan database atau kredenal server analitik dengan benar.
4. (Opsional) Tambahkan beberapa server dari file CSV.

    a. Pilih Server database impor massal dari CSV.

    b. Pilih Unduh templat untuk menyimpan file CSV yang menyertakan templat yang dapat Anda sesuaikan.

    c. Masukkan kredensi koneksi untuk database dan server analitik Anda ke dalam file sesuai dengan template. Contoh berikut menunjukkan bagaimana Anda dapat menyediakan database atau analitik kredenal koneksi server dalam file CSV.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle
 service name,Database,Allow public key retrieval,Use SSL,Trust server
 certificate
```

```
Oracle,192.0.2.1,1521,Login/Password authentication,USER-
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,TRUE
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Simpan file CSV Anda setelah Anda menambahkan kredensi untuk semua database dan server analitik Anda.

d. Pilih Browse, lalu pilih file CSV Anda.

5. Pilih Tambahkan server basis data.
6. Setelah Anda menambahkan kredensi untuk semua server OS, pilih server OS Anda dan pilih Temukan server database.

Setelah Anda menambahkan semua database dan server analitik ke dalam modul pengumpulan data, tambahkan ke inventaris. Modul pengumpulan data database dan analitik dapat terhubung ke server dari inventaris dan mengumpulkan metadata dan metrik kinerja.

Untuk menambahkan database dan server analitik Anda ke inventaris

1. Pada halaman Database dan kolektor analitik, pilih Server database di bawah Discovery di panel navigasi.
2. Pilih database dan server analitik, yang ingin Anda kumpulkan metadata dan metrik kinerjanya.
3. Pilih Tambahkan ke inventaris.

Setelah menambahkan semua server database dan analitik ke inventaris, Anda dapat mulai mengumpulkan metadata dan metrik kinerja. Lihat informasi yang lebih lengkap di Pengumpulan data database dan analitik.

Data yang dikumpulkan oleh database Agentless Collector dan modul pengumpulan data analitik

Modul pengumpulan data database dan analitik Application Discovery Service Agentless Collector (Agentless Collector) mengumpulkan metrik berikut dari lingkungan data Anda. Untuk informasi

tentang pengaturan pengumpulan data, lihatMenggunakan modul pengumpulan data database dan analitik.

Saat Anda menggunakan modul pengumpulan data database dan analitik untuk mengumpulkan Metadata dan kapasitas database, modul ini menangkap metrik berikut.

- Memori yang tersedia di server OS Anda
- Penyimpanan yang tersedia di server OS Anda
- Versi dan edisi basis data
- Jumlah CPUs di server OS Anda
- Jumlah skema
- Jumlah prosedur yang disimpan
- Jumlah tabel
- Jumlah pemicu
- Jumlah tampilan
- Struktur skema

Setelah Anda meluncurkan analisis skema di AWS DMS konsol, modul pengumpulan data Anda menganalisis dan menampilkan metrik berikut.

- Tanggal dukungan basis data
- Jumlah baris kode
- Kompleksitas skema
- Kesamaan skema

Saat Anda menggunakan modul pengumpulan data database dan analitik untuk mengumpulkan Metadata, kapasitas database, dan pemanfaatan sumber daya, modul ini menangkap metrik berikut.

- I/O throughput pada server database Anda
- Operasi input/output per detik (IOPS) di server database Anda
- Jumlah CPUs yang digunakan server OS Anda
- Penggunaan memori di server OS Anda
- Penggunaan penyimpanan di server OS Anda

Anda dapat menggunakan modul pengumpulan data database dan analitik untuk mengumpulkan metadata, kapasitas, dan metrik pemanfaatan dari database Oracle dan SQL Server Anda. Pada saat yang sama, untuk database PostgreSQL dan MySQL, modul pengumpulan data hanya dapat mengumpulkan metadata.

Melihat data yang Anda kumpulkan

> **Important**
>
> Pemberitahuan akhir dukungan: Pada 20 Mei 2026, AWS akan mengakhiri dukungan untuk Penasihat AWS Database Migration Service Armada. Setelah 20 Mei 2026, Anda tidak akan lagi dapat mengakses konsol Penasihat AWS DMS Armada atau sumber daya Penasihat AWS DMS Armada. Untuk informasi lebih lanjut, lihat akhir dukungan AWS DMS Fleet Advisor.

Anda dapat melihat data yang dikumpulkan oleh Application Discovery Service Agentless Collector (Agentless Collector) di konsol Migration Hub dengan mengikuti langkah-langkahnya. Melihat server di AWS Migration Hub konsol

Anda juga dapat melihat metrik yang dikumpulkan untuk database dan server analitik di AWS DMS konsol dengan mengambil langkah-langkah berikut.

Untuk melihat data yang ditemukan oleh modul pengumpulan data database dan analitik di AWS DMS konsol

1. Masuk ke Konsol Manajemen AWS dan buka AWS DMS konsol di https://console.aws.amazon.com/dms/v2/.
2. Pilih Inventaris di bawah Temukan. Halaman Inventaris terbuka.
3. Pilih Analisis inventaris untuk menentukan properti skema database, seperti kesamaan dan kompleksitas.
4. Pilih tab Skema untuk melihat hasil analisis.

Anda dapat menggunakan AWS DMS konsol untuk mengidentifikasi skema duplikat, menentukan kompleksitas migrasi, dan mengekspor informasi inventaris untuk analisis future. Untuk informasi selengkapnya, lihat Menggunakan inventaris untuk analisis di AWS DMS Fleet Advisor.

Mengakses Kolektor Tanpa Agen

Bagian ini menjelaskan cara menggunakan Application Discovery Service Agentless Collector (Agentless Collector).

Topik

- Dasbor Kolektor Tanpa Agen
- Mengedit pengaturan Agentless Collector
- Mengedit VMware kredensi vCenter

Dasbor Kolektor Tanpa Agen

Pada halaman dasbor Application Discovery Service Agentless Collector (Agentless Collector) Anda dapat melihat status kolektor dan memilih metode pengumpulan data seperti yang dijelaskan dalam topik berikut.

Topik

- Status kolektor
- Pengumpulan data

Status kolektor

Status kolektor memberi Anda informasi status tentang kolektor. Nama kolektor, status koneksi kolektor ke AWS, Wilayah beranda Migration Hub, dan versinya.

Jika Anda memiliki masalah AWS koneksi, Anda mungkin perlu mengedit pengaturan konfigurasi Agentless Collector.

Untuk mengedit pengaturan konfigurasi kolektor, pilih Edit pengaturan kolektor dan ikuti instruksi yang dijelaskan diMengedit pengaturan Agentless Collector.

Pengumpulan data

Di bawah Pengumpulan data, Anda dapat memilih metode pengumpulan data. Application Discovery Service Agentless Collector (Agentless Collector) saat ini mendukung pengumpulan data dari VMware VMs dan dari database dan server analitik. Modul masa depan akan mendukung pengumpulan dari platform virtualisasi tambahan, dan pengumpulan tingkat sistem operasi.

Topik

- VMware pengumpulan data vCenter
- Pengumpulan data database dan analitik

VMware pengumpulan data vCenter

Untuk mengumpulkan inventaris server, profil, dan data pemanfaatan dari Anda VMware VMs, siapkan koneksi ke server vCenter Anda. Untuk mengatur koneksi, pilih Siapkan di bagian VMware vCenter dan ikuti petunjuk yang dijelaskan di. Menggunakan modul pengumpulan VMware data vCenter Agentless Collector

Setelah Anda mengatur pengumpulan data vCenter, dari dasbor Anda dapat melakukan hal berikut:

- Lihat status pengumpulan data
- Mulai pengumpulan data
- Hentikan pengumpulan data

> **Note**
>
> Pada halaman dasbor, setelah Anda mengatur pengumpulan data vCenter, tombol Set up di bagian VMwarevCenter diganti dengan informasi status pengumpulan data, tombol Stop pengumpulan data, dan tombol Lihat dan edit.

Pengumpulan data database dan analitik

Anda dapat menjalankan modul pengumpulan data database dan analisis Anda dalam dua mode berikut.

Kapasitas metadata dan database

Modul pengumpulan data mengumpulkan informasi seperti skema, versi, edisi, CPU, memori, dan kapasitas disk dari database dan server analitik Anda. Anda dapat menggunakan informasi yang dikumpulkan ini untuk menghitung rekomendasi target di AWS DMS konsol. Jika basis data sumber Anda dilebih-lebihkan atau kurang disediakan, maka rekomendasi target juga akan dilebih-lebihkan atau direvisi.

Ini adalah mode default.

Metadata, kapasitas database, dan pemanfaatan sumber daya

Selain metadata dan informasi kapasitas database, modul pengumpulan data mengumpulkan metrik pemanfaatan aktual CPU, memori, dan kapasitas disk untuk database dan server analitik. Mode ini memberikan rekomendasi target yang lebih akurat daripada mode default karena rekomendasi didasarkan pada beban kerja database yang sebenarnya. Dalam mode ini, modul pengumpulan data mengumpulkan metrik kinerja setiap menit.

Untuk mulai mengumpulkan metadata dan metrik kinerja dari database dan server analitik

1. Pada halaman Database dan pengumpul analitik, pilih Pengumpulan data di panel navigasi.
2. Dari daftar inventaris Database, pilih database dan server analitik yang ingin Anda kumpulkan metadata dan metrik kinerjanya.
3. Pilih Jalankan pengumpulan data. Kotak dialog tipe pengumpulan data terbuka.
4. Pilih cara mengumpulkan data untuk analisis.

   Jika Anda memilih opsi Metadata, kapasitas database, dan pemanfaatan sumber daya, maka tetapkan periode pengumpulan data. Anda dapat mengumpulkan data selama 7 hari berikutnya atau mengatur rentang Kustom 1-60 hari.
5. Pilih Jalankan pengumpulan data. Halaman pengumpulan data terbuka.
6. Pilih tab Kesehatan koleksi untuk melihat status pengumpulan data.

Setelah menyelesaikan pengumpulan data, modul pengumpulan data Anda akan mengunggah data yang dikumpulkan ke bucket Amazon S3 Anda. Kemudian, Anda dapat melihat data yang dikumpulkan ini seperti yang dijelaskan dalamMelihat data yang Anda kumpulkan.

Mengedit pengaturan Agentless Collector

Anda mengonfigurasi kolektor saat pertama kali menyiapkan Application Discovery Service Agentless Collector (Agentless Collector) seperti yang dijelaskan dalam. Mengkonfigurasi Kolektor Tanpa Agen Prosedur berikut menjelaskan cara mengedit pengaturan konfigurasi Agentless Collector.

Untuk mengedit pengaturan konfigurasi kolektor

- Pilih tombol Edit pengaturan kolektor di dasbor Agentless Collector.

  Pada halaman pengaturan Edit kolektor, lakukan hal berikut:

a. Untuk nama Kolektor, masukkan nama untuk mengidentifikasi kolektor. Nama dapat berisi spasi tetapi tidak dapat berisi karakter khusus.

b. Di bawah AWS Akun tujuan untuk data penemuan, masukkan kunci AWS akses dan kunci rahasia untuk AWS akun yang akan ditentukan sebagai akun tujuan untuk menerima data yang ditemukan oleh kolektor. Untuk informasi tentang persyaratan untuk pengguna IAM, lihatMenyebarkan Application Discovery Service Agentless Collector.

   i. Untuk AWS kunci akses, masukkan kunci akses pengguna IAM AWS akun yang Anda tentukan sebagai akun tujuan.

   ii. Untuk AWS kunci rahasia, masukkan kunci rahasia pengguna IAM AWS akun yang Anda tentukan sebagai akun tujuan.

c. Di bawah kata sandi Agentless Collector, ubah kata sandi yang akan digunakan untuk mengautentikasi akses ke Kolektor Tanpa Agen.

   i. Untuk kata sandi Agentless Collector, masukkan kata sandi yang akan digunakan untuk mengautentikasi akses ke Agentless Collector.

   ii. Untuk Masukkan kembali kata sandi Agentless Collector, untuk verifikasi masukkan kata sandi lagi.

d. Pilih Simpan konfigurasi.

Selanjutnya, Anda akan melihatDasbor Kolektor Tanpa Agen.

Mengedit VMware kredensi vCenter

Untuk mengumpulkan inventaris server, profil, dan data pemanfaatan dari Anda VMware VMs, siapkan koneksi ke server vCenter Anda. Untuk informasi tentang pengaturan koneksi VMware vCenter, lihat. Menggunakan modul pengumpulan VMware data vCenter Agentless Collector

Bagian ini menjelaskan cara mengedit kredenal vCenter.

> **Note**
>
> Sebelum mengedit kredenal vCenter, pastikan Anda dapat memberikan kredensil vCenter dengan izin Baca dan Lihat yang ditetapkan untuk grup Sistem.

Untuk mengedit kredensi VMware vCenter

Pada Melihat detail pengumpulan VMware data halaman, pilih Edit server vCenter.

- Pada halaman Edit vCenter, lakukan hal berikut:

  a. Di bawah kredensi vCenter:

     i. Untuk URL/IP vCenter, masukkan alamat IP host Server VMware vCenter Anda.

     ii. Untuk Nama Pengguna vCenter, masukkan nama pengguna lokal atau domain yang digunakan konektor untuk berkomunikasi dengan vCenter. Untuk pengguna domain, gunakan formulir domain\nama pengguna atau nama pengguna@domain.

     iii. Untuk Kata Sandi vCenter, masukkan kata sandi pengguna lokal atau domain.

  b. Pilih Simpan.

Memperbarui Application Discovery Service Agentless Collector secara manual

Saat Anda mengonfigurasi Application Discovery Service Agentless Collector (Agentless Collector), Anda dapat memilih untuk mengaktifkan pembaruan otomatis seperti yang dijelaskan dalam. Mengkonfigurasi Kolektor Tanpa Agen Jika Anda tidak mengaktifkan pembaruan otomatis, Anda harus memperbarui Agentless Collector secara manual.

Prosedur berikut menjelaskan cara memperbarui Agentless Collector secara manual.

Untuk memperbarui Agentless Collector secara manual

1. Dapatkan file Agentless Collector Open Virtualization Archive (OVA) terbaru.
2. (Opsional) Kami menyarankan Anda menghapus file OVA Agentless Collector sebelumnya, sebelum Anda menerapkan yang terbaru.
3. Ikuti langkah-langkah diMenyebarkan Kolektor Tanpa Agen.

Prosedur sebelumnya hanya memperbarui Kolektor Tanpa Agen. Ini adalah tanggung jawab Anda untuk menjaga OS up to date.

Untuk memperbarui instans Amazon EC2

1. Dapatkan alamat IP dari Agentless Collector dari VMware vCenter.

2. Buka konsol VM kolektor dan masuk **`ec2-user`** menggunakan kata sandi **`collector`** seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

3. Ikuti petunjuk di Perbarui perangkat lunak instans pada AL2 instans Anda di Panduan Pengguna Amazon Linux 2.

Penambalan Langsung Kernel

Agentless Collector version 2

Mesin virtual Agentless Collector versi 2 menggunakan Amazon Linux 2023 seperti yang dijelaskan dalam. Menyebarkan Kolektor Tanpa Agen

Untuk mengaktifkan dan menggunakan Live Patching untuk Amazon Linux 2023, lihat Kernel Live Patching AL2023 di Panduan Pengguna Amazon EC2.

Agentless Collector version 1

Mesin virtual Agentless Collector versi 1 menggunakan Amazon Linux 2 seperti yang dijelaskan dalam. Menyebarkan Kolektor Tanpa Agen

Untuk mengaktifkan dan menggunakan Live Patching untuk Amazon Linux 2, lihat Kernel Live Patching AL2 di Panduan Pengguna Amazon EC2.

Untuk meningkatkan dari Agentless Collector versi 1 ke versi 2

1. Instal OVA Agentless Collector baru dengan menggunakan gambar terbaru.
2. Siapkan kredensil.
3. Hapus alat virtual lama.

Pemecahan Masalah Kolektor Tanpa Agen

Bagian ini berisi topik yang dapat membantu Anda memecahkan masalah yang diketahui dengan Application Discovery Service Agentless Collector (Agentless Collector).

Topik

- Memperbaiki Unable to retrieve manifest or certificate file error
- Mengatasi masalah sertifikasi yang ditandatangani sendiri saat mengonfigurasi sertifikat WinRM
- Memperbaiki Agentless Collector tidak dapat mencapai AWS selama pengaturan
- Memperbaiki masalah sertifikasi yang ditandatangani sendiri saat menghubungkan ke host proxy
- Menemukan kolektor yang tidak sehat
- Memperbaiki masalah alamat IP
- Memperbaiki masalah kredensil vCenter
- Memperbaiki masalah penerusan data dalam modul pengumpulan data database dan analitik
- Memperbaiki masalah koneksi dalam modul pengumpulan data database dan analitik
- Dukungan host ESX mandiri
- Menghubungi AWS Support untuk masalah Agentless Collector

Memperbaiki **`Unable to retrieve manifest or certificate file error`**

Jika Anda menerima kesalahan ini saat mencoba menerapkan OVA dari URL Amazon S3 di UI VMware vCenter, pastikan server vCenter Anda memenuhi persyaratan berikut:

- VMware vCenter Server versi 8.0 update 1 atau yang lebih baru
- VMware vCenter Server 7.0 Pembaruan 3q (ISO Build 23788036) atau yang lebih baru

Mengatasi masalah sertifikasi yang ditandatangani sendiri saat mengonfigurasi sertifikat WinRM

Jika Anda mengaktifkan pemeriksaan sertifikat WinRM, Anda mungkin perlu mengimpor otoritas sertifikat yang ditandatangani sendiri ke Kolektor Tanpa Agen.

Untuk mengimpor otoritas sertifikat yang ditandatangani sendiri

1. Buka konsol web VM kolektor di VMware vCenter dan masuk `ec2-user` seperti `collector` kata sandi seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

2. Pastikan bahwa setiap sertifikat CA yang ditandatangani sendiri yang digunakan untuk menandatangani sertifikat WinRM berada di bawah direktori. `/etc/pki/ca-trust/source/anchors` Contoh:

```
/etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
```

3. Untuk menginstal sertifikat baru, jalankan perintah berikut.

```
sudo update-ca-trust
```

4. Mulai ulang Kolektor Tanpa Agen dengan menjalankan perintah berikut

```
sudo shutdown -r now
```

5. (Opsional) Untuk memverifikasi bahwa sertifikat telah berhasil diimpor, Anda dapat menjalankan perintah berikut.

```
sudo trust list --filter=ca-anchors | less
```

Memperbaiki Agentless Collector tidak dapat mencapai AWS selama pengaturan

Agentless Collector memerlukan akses keluar melalui port TCP 443 ke beberapa domain. AWS Saat mengonfigurasi Agentless Collector di konsol, Anda bisa mendapatkan pesan kesalahan berikut.

> Tidak Bisa Mencapai AWS
>
> AWS tidak dapat dijangkau. Harap verifikasi pengaturan jaringan.

Kesalahan ini terjadi karena upaya yang gagal oleh Agentless Collector untuk membuat koneksi HTTPS ke AWS domain yang kolektor perlu berkomunikasi dengan selama proses penyiapan. Konfigurasi Agentless Collector gagal jika koneksi tidak dapat dibuat.

Untuk memperbaiki koneksi ke AWS

1. Periksa dengan admin TI Anda untuk melihat apakah firewall perusahaan Anda memblokir lalu lintas keluar pada port 443 ke salah satu AWS domain yang memerlukan akses keluar. AWS

Domain mana yang memerlukan akses keluar tergantung pada apakah Wilayah asal Anda adalah Wilayah AS Barat (Oregon), us-west-2, atau Wilayah lainnya.

Domain berikut memerlukan akses keluar jika wilayah beranda AWS akun Anda adalah us-west-2:

- `arsenal-discovery.us-west-2.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Domain berikut memerlukan akses keluar jika wilayah beranda AWS akun Anda tidak: **`us-west-2`**

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.`*`your-home-region`*`.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Jika firewall Anda memblokir akses keluar ke AWS domain yang perlu dikomunikasikan dengan Agentless Collector, konfigurasikan host proxy di bagian Sinkronisasi data di bawah konfigurasi Kolektor.

2. Jika memperbarui firewall tidak menyelesaikan masalah koneksi, gunakan langkah-langkah berikut untuk memastikan bahwa mesin virtual kolektor memiliki konektivitas jaringan keluar ke domain yang tercantum pada langkah sebelumnya.

   a. Dapatkan alamat IP dari Agentless Collector dari VMware vCenter.

   b. Buka konsol web VM kolektor dan masuk **`ec2-user`** menggunakan kata sandi **`collector`** seperti yang ditunjukkan pada contoh berikut.

   ```
   username: ec2-user
   password: collector
   ```

   c. Uji koneksi ke domain yang terdaftar dengan menjalankan telnet pada port 443 seperti yang ditunjukkan pada contoh berikut.

```
telnet migrationhub-config.us-west-2.amazonaws.com 443
```

3. Jika telnet tidak dapat menyelesaikan domain, coba konfigurasikan server DNS statis menggunakan instruksi untuk Amazon Linux 2.
4. Jika kesalahan berlanjut, untuk dukungan lebih lanjut, lihatMenghubungi AWS Support untuk masalah Agentless Collector.

Memperbaiki masalah sertifikasi yang ditandatangani sendiri saat menghubungkan ke host proxy

Jika komunikasi dengan proxy yang disediakan secara opsional melalui HTTPS dan proxy memiliki sertifikat yang ditandatangani sendiri, Anda mungkin perlu memberikan sertifikat.

1. Dapatkan alamat IP dari Agentless Collector dari VMware vCenter.
2. Buka konsol web VM kolektor dan masuk seperti `ec2-user` kata sandi `collector` seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

3. Tempelkan isi sertifikat yang terkait dengan proxy aman, termasuk keduanya `-----BEGIN CERTIFICATE-----` dan`-----END CERTIFICATE-----`, ke dalam file berikut:

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. Untuk menginstal sertifikat baru, jalankan perintah berikut:

```
sudo update-ca-trust
```

5. Mulai ulang kolektor tanpa agen dengan menjalankan perintah berikut:

```
sudo shutdown -r now
```

Menemukan kolektor yang tidak sehat

Informasi status untuk setiap kolektor ditemukan di halaman Pengumpul data konsol AWS Migration Hub (Migration Hub). Anda dapat mengidentifikasi kolektor dengan masalah dengan menemukan kolektor dengan Status Membutuhkan perhatian.

Prosedur berikut menjelaskan cara mengakses konsol Agentless Collector untuk mengidentifikasi masalah kesehatan.

Untuk mengakses konsol Agentless Collector

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Pengumpul data.
3. Dari tab Agentless collectors, catat alamat IP untuk setiap konektor yang berstatus Membutuhkan perhatian.
4. Untuk membuka konsol Agentless Collector, buka browser web. Kemudian ketik URL berikut di bilah alamat: **`https://`** *`<ip_address>`***`/`**, di mana ip_address adalah alamat IP kolektor yang tidak sehat.
5. Pilih Masuk, lalu masukkan kata sandi Agentless Collector, yang diatur saat kolektor dikonfigurasi. Mengkonfigurasi Kolektor Tanpa Agen
6. Pada halaman dasbor Agentless Collector, di bawah Pengumpulan data, pilih Lihat dan edit di bagian vCenterVMware .
7. Ikuti petunjuk Mengedit VMware kredensi vCenter untuk memperbaiki URL dan kredensialnya.

Setelah memperbaiki masalah kesehatan, kolektor akan membangun kembali konektivitas dengan server vCenter, dan status kolektor akan berubah ke status Collecting. Jika masalah berlanjut, lihatMenghubungi AWS Support untuk masalah Agentless Collector.

Penyebab paling umum untuk kolektor yang tidak sehat adalah alamat IP dan masalah kredensional. Memperbaiki masalah alamat IPdan Memperbaiki masalah kredensil vCenter dapat membantu Anda menyelesaikan masalah ini dan mengembalikan kolektor ke keadaan sehat.

Memperbaiki masalah alamat IP

Seorang kolektor dapat masuk ke keadaan tidak sehat jika titik akhir vCenter yang disediakan selama penyiapan kolektor salah bentuk, tidak valid, atau jika server vCenter saat ini sedang down dan tidak dapat dijangkau. Dalam hal ini, Anda akan menerima pesan kesalahan Koneksi.

Prosedur berikut dapat membantu Anda menyelesaikan masalah alamat IP.

Untuk memperbaiki masalah alamat IP kolektor

1. Dapatkan alamat IP dari Agentless Collector dari VMware vCenter.
2. Buka konsol Agentless Collector dengan membuka browser web, lalu ketik URL berikut di bilah alamat: **`https://`** *`<ip_address>`***`/`**, di mana ip_address adalah alamat IP kolektor. Menyebarkan Kolektor Tanpa Agen
3. Pilih Masuk, lalu masukkan kata sandi Agentless Collector, yang diatur saat kolektor dikonfigurasi. Mengkonfigurasi Kolektor Tanpa Agen
4. Pada halaman dasbor Agentless Collector, di bawah Pengumpulan data, pilih Lihat dan edit di bagian vCenterVMware .
5. Pada halaman rincian pengumpulan VMware data, di bawah server vCenter Ditemukan, catat alamat IP di kolom vCenter.
6. Menggunakan alat baris perintah terpisah seperti `ping` ata`utraceroute`, validasi bahwa server vCenter terkait aktif dan IP dapat dijangkau dari VM kolektor.

    - Jika alamat IP salah dan layanan vCenter aktif, maka perbarui alamat IP di konsol kolektor, dan pilih Berikutnya.
    - Jika alamat IP benar tetapi server vCenter tidak aktif, aktifkan.
    - Jika alamat IP benar dan server vCenter aktif, periksa apakah itu memblokir masuknya koneksi jaringan karena masalah firewall. Jika ya, perbarui pengaturan firewall Anda untuk memungkinkan koneksi masuk dari kolektor VM.

Memperbaiki masalah kredensil vCenter

Kolektor dapat masuk ke keadaan tidak sehat jika kredensi pengguna vCenter yang disediakan saat mengkonfigurasi kolektor tidak valid, atau tidak memiliki hak akses akun vCenter Baca dan Lihat.

Jika Anda mengalami masalah yang terkait dengan kredenal vCenter, periksa untuk memastikan bahwa Anda memiliki izin Baca dan Tampilan vCenter yang disetel untuk grup Sistem.

Untuk informasi tentang mengedit kredenal vCenter, lihat. Mengedit VMware kredensi vCenter

Memperbaiki masalah penerusan data dalam modul pengumpulan data database dan analitik

Halaman beranda modul pengumpulan data database dan analitik di Agentless Collector menampilkan status koneksi untuk Akses ke DMS dan Akses ke S3. Jika Anda melihat Tidak ada akses untuk Akses ke DMS dan Akses ke S3, maka konfigurasikan penerusan data. Untuk informasi selengkapnya, lihat Mengkonfigurasi penerusan data.

Jika Anda mengalami masalah ini setelah mengonfigurasi penerusan data, periksa untuk memastikan bahwa modul pengumpulan data Anda dapat mengakses ke internet. Kemudian, pastikan Anda menambahkan DMSCollectorkebijakan Policy dan FleetAdvisorS3Policy ke pengguna IAM Anda. Untuk informasi selengkapnya, lihat Menyebarkan Application Discovery Service Agentless Collector.

Jika modul pengumpulan data Anda tidak dapat terhubung AWS, berikan akses keluar ke domain berikut.

- `dms.`*`your-home-region`*`.amazonaws.com`
- `s3.amazonaws.com`

Memperbaiki masalah koneksi dalam modul pengumpulan data database dan analitik

Modul pengumpulan data database dan analitik di Agentless Collector terhubung ke server LDAP Anda untuk menemukan server OS di lingkungan data Anda. Kemudian, modul pengumpulan data terhubung ke server OS Anda untuk menemukan server database dan analitik. Dari server database ini, modul pengumpulan data mengumpulkan metrik kapasitas dan kinerja. Jika modul pengumpulan data Anda tidak dapat terhubung ke server ini, maka verifikasi bahwa Anda dapat terhubung ke server Anda.

Dalam contoh berikut, ganti *`replaceable`* nilai dengan nilai Anda.

- Untuk memverifikasi bahwa Anda dapat terhubung ke server LDAP Anda, instal `ldap-util` paket. Untuk melakukannya, jalankan perintah berikut.

```
sudo apt-get install ldap-util
```

Kemudian, jalankan perintah berikut.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b
 "dc=example,dc=com" -h
```

- Untuk memverifikasi bahwa Anda dapat terhubung ke server OS Linux, gunakan perintah berikut.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Jalankan contoh sebelumnya sebagai administrator di Windows.

```
ssh username@my-linux-host.domain.com
```

Jalankan contoh sebelumnya di Linux.

- Untuk memverifikasi bahwa Anda dapat terhubung ke server OS Windows, gunakan perintah berikut.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Jalankan contoh sebelumnya sebagai administrator di Windows.

```
sudo apt install -y winrm
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]
 "[cmd.exe or any other CLI command]"
```

Jalankan contoh sebelumnya di Linux.

- Untuk memverifikasi bahwa Anda dapat terhubung ke database SQL Server, gunakan perintah berikut.

```
sqlcmd -S [hostname or IP] -U username -P 'password'
SELECT GETDATE() AS sysdate
```

- Untuk memverifikasi bahwa Anda dapat terhubung ke database MySQL, gunakan perintah berikut.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]
SELECT NOW() FROM DUAL
```

- Untuk memverifikasi bahwa Anda dapat terhubung ke database Oracle, gunakan perintah berikut.

```
sqlplus username/password@[hostname or IP]:port/servicename
SELECT SYSDATE FROM DUAL
```

- Untuk memverifikasi bahwa Anda dapat terhubung ke database PostgreSQL, gunakan perintah berikut.

```
psql -U username -h [hostname or IP] -p port -d database
SELECT CURRENT_TIMESTAMP AS sysdate
```

Jika Anda tidak dapat terhubung ke database dan server analitik, pastikan Anda memberikan izin yang diperlukan. Untuk informasi selengkapnya, lihat Menemukan server database Anda.

Dukungan host ESX mandiri

Agentless Collector tidak mendukung host ESX mandiri. Host ESX harus menjadi bagian dari instans Server vCenter.

Menghubungi AWS Support untuk masalah Agentless Collector

Jika Anda mengalami masalah dengan Application Discovery Service Agentless Collector (Agentless Collector) dan membutuhkan bantuan, hubungi AWS Support Anda akan dihubungi dan mungkin diminta untuk mengirim log kolektor.

Untuk mendapatkan log Kolektor Tanpa Agen

1. Dapatkan alamat IP dari Agentless Collector dari VMware vCenter.
2. Buka konsol web VM kolektor dan masuk **`ec2-user`** menggunakan kata sandi **`collector`** seperti yang ditunjukkan pada contoh berikut.

```
username: ec2-user
password: collector
```

3. Gunakan perintah berikut untuk menavigasi ke folder log.

```
cd /var/log/aws/collector
```

4. Zip file log dengan menggunakan perintah berikut.

```
sudo cp /local/agentless_collector/compose.log .
```

```
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/
dev/null
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz --exclude='db.mv*' *
```

5. Salin file log dari VM Agentless Collector.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Berikan `tar.gz` file ke AWS Enterprise Support.

Mengimpor data ke Migration Hub

AWS Migration Hub Impor (Migration Hub) memungkinkan Anda mengimpor detail lingkungan lokal langsung ke Migration Hub tanpa menggunakan Application Discovery Service Agentless Collector (Agentless Collector) atau Agen Penemuan AWS Aplikasi (Agen Penemuan), sehingga Anda dapat melakukan penilaian dan perencanaan migrasi langsung dari data yang diimpor. Anda juga dapat mengelompokkan perangkat sebagai aplikasi dan melacak status migrasinya.

Halaman ini menjelaskan langkah-langkah untuk menyelesaikan permintaan impor. Pertama, Anda menggunakan salah satu dari dua opsi berikut untuk menyiapkan data server lokal Anda.

- Gunakan alat pihak ketiga yang umum untuk membuat file yang berisi data server lokal Anda.
- Unduh templat impor nilai dipisahkan koma (CSV) kami, dan isi dengan data server lokal Anda.

Setelah menggunakan salah satu dari dua metode yang dijelaskan sebelumnya untuk membuat file data lokal, Anda mengunggah file ke Hub Migrasi menggunakan konsol Hub Migrasi AWS CLI, atau salah satunya. AWS SDKs Untuk informasi lebih lanjut tentang dua opsi, lihatthe section called “Format impor yang didukung”.

Anda dapat mengirimkan beberapa permintaan impor. Setiap permintaan diproses secara berurutan. Anda dapat memeriksa status permintaan impor Anda kapan saja, melalui konsol atau impor APIs.

Setelah permintaan impor selesai, Anda dapat melihat detail tiap catatan yang diimpor. Lihat data penggunaan, tag, dan pemetaan aplikasi langsung dari dalam konsol Migration Hub. Jika terjadi kesalahan saat mengimpor, Anda dapat meninjau jumlah catatan keberhasilan dan kegagalan, lalu Anda dapat melihat detail kesalahan untuk setiap catatan kegagalan.

Menangani kesalahan: Disediakan sebuah tautan untuk mengunduh log kesalahan dan file catatan kegagalan dengan format file CSV dalam arsip terkompresi. Gunakan file-file ini untuk mengirimkan ulang permintaan impor Anda setelah mengoreksi kesalahan.

Ada batas penyimpanan yang berlaku untuk jumlah catatan yang diimpor, server yang diimpor, dan catatan yang dihapus. Untuk informasi selengkapnya, lihat AWS Application Discovery Service Kuota.

Format impor yang didukung

Migration Hub mendukung format impor berikut.

- RVTools
- Templat impor Hub Migrasi

RVTools

Migration Hub mendukung impor ekspor vSphere melalui VMware . RVTools Saat menyimpan data dari RVTools, pertama-tama pilih Ekspor semua ke csv opsi atau Ekspor semua ke Excel opsi, lalu ZIP folder, dan impor file ZIP ke Migration Hub. File-file berikut diperlukan dalam ZIP: vInfo, vNetwork, vCPU, vMemory, vDisk, vPartition, vSource, VTools, vHost, VNIC, VSC_VMK.

Templat impor Hub Migrasi

Impor Migration Hub memungkinkan Anda mengimpor data dari sumber mana pun. Data yang diberikan harus dalam format yang didukung untuk file CSV, dan data tersebut harus hanya berisi bidang yang didukung dengan rentang yang didukung untuk bidang tersebut.

Tanda bintang (*) di samping nama bidang impor dalam tabel berikut menunjukkan bahwa itu adalah bidang wajib. Setiap catatan file impor Anda harus memiliki setidaknya satu atau lebih bidang yang diperlukan ini dalam keadaan terisi untuk mengidentifikasi server atau aplikasi secara unik. Jika tidak, catatan tanpa salah satu bidang yang diperlukan akan gagal diimpor.

Tanda sisipan (^) di samping nama file impor dalam tabel berikut menunjukkan bahwa itu adalah readonly jika ServerID disediakan.

> **Note**
>
> Jika Anda menggunakan keduanya VMware. MoRefId atau VMWare. VCenterId, untuk mengidentifikasi catatan, Anda harus memiliki kedua bidang dalam catatan yang sama.

Nama Bidang Impor	Deskripsi	Contoh
ExternalId*^	Pengenal kustom yang memungkinkan Anda menandai setiap rekaman sebagai entri unik. Misalnya, ExternalIdbisa menjadi ID	Id inventaris 1 Server 2 Id CMBD 3

Nama Bidang Impor	Deskripsi	Contoh
	inventaris untuk server di pusat data Anda.	
SMBiosId ^	ID BIOS manajemen sistem (SMBIOS).	
IPAddress*^	Daftar alamat IP server yang dipisahkan koma, dalam tanda kutip.	192.0.0.2 “10.12.31.233, 10.12.32.11"
MACAddress*^	Daftar alamat MAC server yang dipisahkan koma, dalam tanda kutip.	00:1B:44:11:3A:B7 “00-15-E9-2B-99-3C, 00-14-22-01-23-45"
HostName*^	Nama host server. Kami merekomendasikan untuk menggunakan nama domain yang memenuhi syarat (FQDN) untuk nilai ini.	ip-1-2-3-4 localhost.domain
VMware.MoRefId*^	ID referensi objek terkelola . Harus dilengkapi dengan a VMware. VCenterId.	
VMware. VCenterId*^	Pengenal unik mesin virtual. Harus dilengkapi dengan a VMware. MoRefId.	
CPU. NumberOfProcessors^	Jumlah CPUs.	4
CPU. NumberOfCores^	Jumlah total inti fisik.	8

Nama Bidang Impor	Deskripsi	Contoh
CPU. NumberOfLogicalCores^	Jumlah total thread yang dapat berjalan secara bersamaan pada semua CPUs di server. Beberapa CPUs mendukung beberapa utas untuk berjalan secara bersamaan pada satu inti CPU. Dalam kasus tersebut, jumlah ini akan lebih besar dari jumlah inti fisik (atau virtual).	16
OS.nama^	Nama sistem operasi.	Linux Windows.Hat
OS.versi^	Versi sistem operasi.	16.04.3 NT 6.2.8
VMware.VMName^	Nama mesin virtual.	Corp1
DOMBA JANTAN. TotalSize InMB^	Total RAM yang tersedia di server, dalam satuan MB.	64 128
DOMBA JANTAN. UsedSizeI nMB.AVG^	Jumlah rata-rata RAM yang digunakan pada server, dalam satuan MB.	64 128
DOMBA JANTAN. UsedSizeI nMB.maks^	Jumlah rata-rata RAM yang digunakan pada server, dalam satuan MB.	64 128
CPU. UsagePct.Avg^	Rata-rata penggunaan CPU saat alat penemuan mengumpulkan data.	45 23.9

Nama Bidang Impor	Deskripsi	Contoh
CPU. UsagePct.Maks^	Penggunaan maksimum CPU saat alat penemuan mengumpulkan data.	55,34 24
DiskReadsPerSecond lnKB.AVG^	Jumlah rata-rata informasi yang dibaca disk per detik, dalam satuan KB.	1159 84506
DiskWritesPerSecon dInKB.AVG^	Jumlah rata-rata informasi yang ditulis disk per detik, dalam satuan KB.	199 6197
DiskReadsPerSecond lnKb.maks^	Jumlah maksimum informasi yang dibaca disk per detik, dalam satuan KB.	37892 869962
DiskWritesPerSecon dInKb.maks^	Jumlah maksimum informasi yang ditulis disk per detik, dalam satuan KB.	18436 1808
DiskReadsOpsPerSec ond.Avg^	Jumlah rata-rata operasi pembacaan disk per detik.	45 28
DiskWritesOpsPerSe cond.Avg^	Jumlah rata-rata operasi penulisan disk per detik.	8 3
DiskReadsOpsPerSec ond.Maks^	Jumlah maksimum operasi pembacaan disk per detik.	1083 176
DiskWritesOpsPerSe cond.Maks^	Jumlah maksimum operasi penulisan disk per detik.	535 71

Nama Bidang Impor	Deskripsi	Contoh
NetworkReadsPerSecondInKB.AVG^	Jumlah rata-rata operasi pembacaan jaringan per detik, dalam satuan KB.	45 28
NetworkWritesPerSecondInKB.AVG^	Jumlah rata-rata operasi penulisan jaringan per detik, dalam satuan KB.	8 3
NetworkReadsPerSecondInKb.maks^	Jumlah maksimum operasi pembacaan jaringan per detik, dalam satuan KB.	1083 176
NetworkWritesPerSecondInKb.maks^	Jumlah maksimum operasi penulisan jaringan per detik, dalam satuan KB.	535 71
Aplikasi	Daftar dipisahkan koma berisi aplikasi yang mencakup server ini, dalam tanda kutip. Nilai ini dapat mencakup aplikasi yang ada aplikasi and/or baru yang dibuat pada saat impor.	Aplikasi1 “Aplikasi2, Aplikasi3"
ApplicationWave	Gelombang migrasi untuk server ini.	

Nama Bidang Impor	Deskripsi	Contoh
Tag^	Daftar dipisahkan koma berisi tag yang diformat sebagai nama:nilai. **Important** Jangan menyimpan informasi sensitif (seperti data pribadi) di tag.	“zona:1, penting:ya” “zona:3, penting:tidak, zona:1"
ServerId	Pengidentifikasi server seperti yang terlihat dalam daftar server Migration Hub.	`d-server-01kk9i6yw waxmp`

Anda dapat mengimpor data meskipun tidak semua bidang yang ditentukan dalam templat impor berisi data, asalkan setiap catatan memiliki setidaknya salah satu bidang yang diperlukan di dalamnya. Duplikat dikelola di beberapa permintaan impor dengan menggunakan kunci pencocokan eksternal atau internal. Jika Anda mengisi sendiri kunci pencocokan, `External ID`, bidang ini digunakan untuk mengidentifikasi dan mengimpor catatan secara unik. Jika tidak ada kunci pencocokan yang ditentukan, impor akan menggunakan kunci pencocokan yang dihasilkan secara internal yang berasal dari beberapa kolom dalam templat impor. Untuk informasi lebih lanjut tentang pencocokan ini, lihat Logika pencocokan untuk server dan aplikasi yang ditemukan.

Note

Impor Migration Hub tidak mendukung bidang apa pun di luar yang ditentukan dalam templat impor. Bidang kustom apa pun yang disediakan akan diabaikan dan tidak akan diimpor.

Menyiapkan izin impor

Sebelum Anda dapat mengimpor data, pastikan bahwa pengguna IAM Anda memiliki izin Amazon S3 yang diperlukan untuk mengunggah `s3:PutObject` () file impor Anda ke Amazon S3, dan untuk

membaca objek (). `s3:GetObject` Anda juga harus membuat akses terprogram (untuk AWS CLI) atau akses konsol, dengan membuat kebijakan IAM dan melampirkannya ke pengguna IAM yang melakukan impor di akun Anda. AWS

Console Permissions

Gunakan prosedur berikut untuk mengedit kebijakan izin untuk pengguna IAM yang akan membuat permintaan impor di AWS akun Anda menggunakan konsol.

Untuk mengedit kebijakan terkelola yang dilampirkan pada pengguna

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna.
3. Pilih nama pengguna yang memiliki kebijakan izin yang ingin Anda ubah.
4. Pilih tab Izin, lalu pilih Tambahkan izin.
5. Pilih Lampirkan kebijakan yang ada, lalu pilih Buat kebijakan.

    a. Pada halaman Buat kebijakan yang terbuka, pilih JSON, dan tempelkan kebijakan berikut. Ingatlah untuk mengganti nama bucket Anda dengan nama aktual bucket yang akan menjadi tujuan pengunggahan file impor oleh pengguna IAM.

    JSON

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

```
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

b. Pilih Tinjau kebijakan.

c. Beri Nama baru dan deskripsi opsional pada kebijakan Anda, sebelum meninjau ringkasan kebijakan.

d. Pilih Buat kebijakan.

6. Kembali ke halaman konsol IAM izin hibah untuk pengguna yang akan membuat permintaan impor di akun Anda AWS .
7. Segarkan tabel kebijakan, dan cari nama kebijakan yang baru saja Anda buat.
8. Pilih Berikutnya: Tinjauan.
9. Pilih Tambahkan izin.

Setelah menambahkan kebijakan ke pengguna IAM, Anda siap untuk memulai proses impor.

AWS CLI Permissions

Gunakan prosedur berikut untuk membuat kebijakan terkelola yang diperlukan untuk memberi pengguna IAM izin untuk membuat permintaan data impor menggunakan. AWS CLI

Untuk membuat dan melampirkan kebijakan terkelola

1. Gunakan `aws iam create-policy` AWS CLI perintah untuk membuat kebijakan IAM dengan izin berikut. Ingatlah untuk mengganti nama bucket Anda dengan nama aktual bucket yang akan menjadi tujuan pengunggahan file impor oleh pengguna IAM.

   JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

Untuk informasi selengkapnya tentang menggunakan perintah ini, lihat buat-kebijakan dalam Refensi Perintah AWS CLI .

2. Gunakan `aws iam create-policy` AWS CLI perintah untuk membuat kebijakan IAM tambahan dengan izin berikut.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "discovery:ListConfigurations",
                "discovery:CreateApplication",
                "discovery:UpdateApplication",
                "discovery:AssociateConfigurationItemsToApplication",
                "discovery:DisassociateConfigurationItemsFromApplication",
                "discovery:GetDiscoverySummary",
                "discovery:StartImportTask",
                "discovery:DescribeImportTasks",
                "discovery:BatchDeleteImportData"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

3. Gunakan `aws iam attach-user-policy` AWS CLI perintah untuk melampirkan kebijakan yang Anda buat dalam dua langkah sebelumnya ke pengguna IAM yang akan melakukan permintaan impor di AWS akun Anda menggunakan. AWS CLI Untuk informasi selengkapnya tentang penggunaan perintah ini, lihat attach-user-policydi AWS CLI Command Reference.

Sekarang setelah Anda menambahkan kebijakan ke pengguna IAM Anda, Anda siap untuk memulai proses impor.

Ingatlah bahwa ketika pengguna IAM mengunggah objek ke bucket Amazon S3 yang Anda tentukan, mereka harus meninggalkan izin default untuk objek yang disetel sehingga pengguna dapat membaca objek tersebut.

Mengunggah file impor Anda ke Amazon S3

Selanjutnya, Anda harus mengunggah file impor berformat CSV ke Amazon S3 sehingga dapat diimpor. Sebelum Anda mulai, Anda harus memiliki bucket Amazon S3 yang akan menampung file impor Anda yang dibuat and/or dipilih sebelumnya.

Console S3 Upload

Untuk mengunggah file impor ke Amazon S3

1. Masuk ke Konsol Manajemen AWS dan buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Di daftar Nama bucket, pilih nama bucket tujuan penunggahan objek Anda.
3. Pilih Unggah.
4. Di kotak dialog Unggah, pilih Tambahkan file untuk memilih file yang akan diunggah.
5. Pilih file yang akan diunggah, lalu pilih Buka.
6. Pilih Unggah.
7. Setelah file Anda diunggah, pilih nama objek file data Anda dari dasbor bucket Anda.
8. Dari tab Gambaran Umum pada halaman detail objek, salin URL objek. Anda akan memerlukannya saat membuat permintaan impor.

9. Buka halaman Impor di konsol Migration Hub seperti yang dijelaskan diMengimpor data. Kemudian, tempel URL objek di bidang URL Objek Amazon S3.

AWS CLI S3 Upload

Untuk mengunggah file impor ke Amazon S3

1. Buka jendela terminal dan arahkan ke direktori tempat file impor Anda disimpan.
2. Masukkan perintah berikut:

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Ini mengembalikan hasil berikut:

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Salin jalur lengkap objek Amazon S3 yang dihasilkan. Anda akan membutuhkan ini ketika Anda membuat permintaan impor Anda.

Mengimpor data

Setelah mengunduh templat impor dari konsol Migration Hub dan mengisinya dengan data server lokal yang ada, Anda siap untuk mulai mengimpor data ke Migration Hub. Petunjuk berikut menjelaskan dua cara untuk melakukan ini, baik dengan menggunakan konsol atau dengan melakukan panggilan API melalui AWS CLI.

Console Import

Mulai impor data pada halaman Alat di konsol Migration Hub.

Untuk memulai impor data

1. Pada panel navigasi, di bawah Temukan, pilih Alat.
2. Jika Anda belum memiliki templat impor yang terisi, Anda dapat mengunduh templat dengan memilih templat impor di kotak Impor. Buka templat yang diunduh dan isi dengan data server on-premise yang ada. Anda juga dapat mengunduh template impor dari bucket Amazon S3 kami di import_template.csv https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/

3. Untuk membuka halaman Impor, pilih Impor di kotak Impor.
4. Di bawah Impor nama, tentukan nama untuk impor.
5. Isi bidang URL Objek Amazon S3. Untuk melakukan langkah ini, Anda harus mengunggah file data impor ke Amazon S3. Untuk informasi selengkapnya, lihat Mengunggah file impor Anda ke Amazon S3.
6. Pilih Impor di area kanan bawah. Ini akan membuka halaman Impor tempat Anda dapat melihat impor dan statusnya tercantum dalam tabel.

Setelah mengikuti prosedur sebelumnya untuk memulai impor data, halaman Impor akan menampilkan detail setiap permintaan impor termasuk status progres, waktu penyelesaian, dan jumlah catatan keberhasilan atau kegagalan dengan kemampuan mengunduh catatan tersebut. Dari layar ini, Anda juga dapat berpindah ke halaman Server di bagian Temukan untuk melihat data aktual yang diimpor.

Pada halaman Server, Anda dapat melihat daftar semua server (perangkat) yang ditemukan beserta nama impornya. Saat Anda menavigasi dari halaman Impor (riwayat impor) dengan memilih nama impor yang tercantum di kolom Nama, Anda akan dibawa ke halaman Server tempat filter diterapkan berdasarkan kumpulan data impor yang dipilih. Kemudian, Anda hanya melihat data milik impor tertentu.

Arsip dalam format .zip dan berisi dua file: `errors-file` dan `failed-entries-file`. File kesalahan berisi daftar pesan kesalahan yang terkait dengan setiap baris gagal dan nama kolom terkait dari file data Anda yang gagal diimpor. Anda dapat menggunakan file ini untuk dengan cepat mengidentifikasi letak masalah. File entri gagal mencakup setiap baris dan semua kolom yang disediakan yang gagal. Anda dapat membuat perubahan yang disebutkan dalam file kesalahan ini dan mencoba mengimpor file lagi dengan informasi yang telah dikoreksi.

AWS CLI Import

Untuk memulai proses impor data dari AWS CLI, pertama-tama AWS CLI harus diinstal di lingkungan Anda. Untuk informasi selengkapnya, lihat Menginstal Antarmuka Baris AWS Perintah di Panduan AWS Command Line Interface Pengguna.

> **Note**
>
> Jika Anda belum memiliki template impor yang diisi, Anda dapat mengunduh template impor dari bucket Amazon S3 kami di sini: import_template.csv https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/

Untuk memulai impor data

1. Buka jendela terminal, dan ketik perintah berikut:

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --
name ImportName
```

2. Langkah ini akan membuat tugas impor Anda dan menghasilkan informasi status berikut:

```
{
    "task": {
        "status": "IMPORT_IN_PROGRESS",
        "applicationImportSuccess": 0,
        "serverImportFailure": 0,
        "serverImportSuccess": 0,
        "name": "ImportName",
        "importRequestTime": 1547682819.801,
        "applicationImportFailure": 0,
        "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
        "importUrl": "s3://BucketName/ImportFile.csv",
        "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"
    }
}
```

Melacak permintaan impor Hub Migrasi

Anda dapat melacak status permintaan impor Hub Migrasi menggunakan konsol AWS CLI, atau salah satu permintaan impor AWS SDKs.

Console Tracking

Dari dasbor Impor di konsol Migration Hub, Anda akan menemukan elemen berikut.

- Nama – Nama permintaan impor.
- ID Impor – ID unik dari permintaan impor.
- Waktu impor – Tanggal dan waktu permintaan impor dibuat.
- Status impor – Status permintaan impor. Status ini dapat berupa salah satu dari nilai berikut:
  - Sedang mengimpor – File data ini saat ini sedang diimpor.
  - Diimpor – Seluruh file data berhasil diimpor.

  - Diimpor dengan kesalahan – Satu atau beberapa catatan dalam file data gagal diimpor. Untuk mengatasi catatan kegagalan, pilih Unduh catatan kegagalan untuk tugas impor Anda dan selesaikan kesalahan dalam file csv entri yang gagal, dan lakukan impor ulang.
  - Gagal Impor – Tak satu pun dari catatan dalam file data berhasil diimpor. Untuk mengatasi catatan kegagalan, pilih Unduh catatan kegagalan untuk tugas impor Anda dan selesaikan kesalahan dalam file csv entri yang gagal, dan lakukan impor ulang.
- Catatan diimpor – Jumlah catatan dalam file data tertentu yang berhasil diimpor.
- Catatan kegagalan – Jumlah catatan dalam file data tertentu yang tidak berhasil diimpor.

CLI Tracking

Anda dapat melacak status tugas impor Anda dengan `aws discovery describe-import-tasks` AWS CLI perintah.

1. Buka jendela terminal, dan ketik perintah berikut:

   ```
   aws discovery describe-import-tasks
   ```

2. Langkah ini akan menghasilkan daftar semua tugas impor Anda dalam format JSON, lengkap dengan status dan informasi lain yang relevan. Atau, Anda dapat memfilter hasil agar menghasilkan subset tugas impor Anda.

Saat melacak tugas impor, Anda mungkin mendapati bahwa nilai `serverImportFailure` yang dihasilkan lebih besar dari nol. Ketika ini terjadi, file impor Anda memiliki satu atau beberapa entri yang tidak dapat diimpor. Hal ini dapat diatasi dengan mengunduh arsip catatan kegagalan, meninjau file di dalamnya, dan melakukan permintaan impor lain dengan file failed-entries.csv yang telah dimodifikasi.

Setelah membuat tugas impor, Anda dapat melakukan tindakan tambahan untuk membantu mengelola dan melacak migrasi data Anda. Misalnya, Anda dapat mengunduh arsip catatan kegagalan untuk permintaan tertentu. Untuk informasi tentang menggunakan arsip catatan kegagalan untuk menyelesaikan masalah impor, lihat Memecahkan masalah catatan impor yang gagal.

Lihat dan jelajahi data yang ditemukan

Baik Application Discovery Service Agentless Collector (Agentless Collector) dan AWS Discovery Agent (Discovery Agent) menyediakan data kinerja sistem berdasarkan pemanfaatan rata-rata dan puncak. Anda dapat menggunakan data kinerja sistem yang dikumpulkan untuk melakukan total biaya kepemilikan (TCO) tingkat tinggi. Discovery Agents mengumpulkan data yang lebih terperinci termasuk data deret waktu untuk informasi performa sistem, koneksi jaringan inbound dan outbound, dan proses yang sedang berjalan di server. Anda dapat menggunakan data ini untuk memahami dependensi jaringan antarserver dan mengelompokkan server terkait sebagai aplikasi untuk perencanaan migrasi.

Di bagian ini Anda akan menemukan petunjuk tentang cara melihat dan bekerja dengan data yang ditemukan oleh Agentless Collector dan Discovery Agent dari konsol dan. AWS CLI

Topik

- Melihat data yang dikumpulkan menggunakan konsol Migration Hub
- Menjelajahi data di Amazon Athena

Melihat data yang dikumpulkan menggunakan konsol Migration Hub

Untuk Application Discovery Service Agentless Collector (Agentless Collector) dan AWS Discovery Agent (Discovery Agent), setelah proses pengumpulan data dimulai, Anda dapat menggunakan konsol untuk melihat data yang dikumpulkan tentang server Anda dan. VMs Data muncul di konsol tersebut sekitar 15 menit setelah pengumpulan data dimulai. Anda juga dapat melihat data ini dalam format CSV dengan mengekspor data yang dikumpulkan dengan melakukan panggilan API menggunakan file. AWS CLI

Untuk melihat data yang dikumpulkan tentang server yang ditemukan di konsol, ikuti langkah-langkahnyaMelihat server di AWS Migration Hub konsol. Untuk mempelajari selengkapnya tentang penggunaan konsol untuk melihat, mengurutkan, dan menandai server yang ditemukan oleh Kolektor Tanpa Agen atau Agen Penemuan, lihat. Menemukan data dengan konsol AWS Migration Hub

Database Agentless Collector dan modul pengumpulan data analitik mengunggah data yang dikumpulkan ke bucket Amazon S3. Anda dapat melihat data dari bucket ini di konsol AWS DMS.

Untuk melihat data yang dikumpulkan tentang database yang ditemukan dan server analitik, ikuti langkah-langkahnyaMelihat data yang Anda kumpulkan.

Logika pencocokan untuk server dan aplikasi yang ditemukan

AWS Application Discovery Service (Application Discovery Service) memiliki logika pencocokan bawaan yang mengidentifikasi kapan server yang ditemukan cocok dengan entri yang ada. Ketika logika ini menemukan kecocokan, informasi untuk server yang sudah ditemukan akan diperbarui dengan nilai-nilai baru.

Logika pencocokan ini menangani duplikat server dari berbagai sumber termasuk impor AWS Migration Hub (Migration Hub), Application Discovery Service Agentless Collector (Agentless Collector), AWS Application Discovery Agent (Discovery Agent), dan alat migrasi lainnya. Untuk informasi selengkapnya tentang impor Hub Migrasi, lihat Impor Hub Migrasi.

Ketika penemuan server berlangsung, setiap entri diperiksa silang dengan catatan yang telah diimpor sebelumnya untuk memastikan bahwa server yang diimpor belum ada. Jika tidak ditemukan kecocokan, catatan baru dibuat dan pengenal server unik baru ditetapkan. Jika ditemukan kecocokan, entri baru masih akan dibuat, tetapi ditugaskan ke pengenal server unik yang sama sebagai server yang sudah ada. Saat melihat server ini di konsol Migration Hub, Anda hanya menemukan satu entri unik untuk server.

Atribut server yang terkait dengan entri ini digabung untuk menunjukkan nilai atribut dari catatan yang tersedia sebelumnya serta catatan yang baru diimpor. Jika ada lebih dari satu nilai untuk atribut server tertentu dari beberapa sumber, misalnya, terdapat dua nilai yang berbeda untuk `Total RAM` yang terkait dengan server tertentu yang ditemukan menggunakan impor dan juga Discovery Agent, maka nilai yang paling terakhir diperbarui akan ditampilkan dalam catatan kecocokan untuk server.

Bidang pencocokan

Bidang berikut digunakan untuk mencocokkan server saat alat penemuan digunakan.

- ExternalId— Ini adalah bidang utama yang digunakan untuk mencocokkan server. Jika nilai dalam bidang ini sama persis dengan `ExternalId` dalam entri lain, maka Application Discovery Service akan mencocokkan kedua entri tersebut, terlepas dari apakah bidang lainnya itu cocok atau tidak.
- IPAddress
- HostName
- MacAddress

- VMware. MoRefIddan VMware. vCenterId Kedua nilai ini harus identik dengan bidang masing-masing di entri lain untuk Application Discovery Service untuk melakukan kecocokan.

Menjelajahi data di Amazon Athena

Eksplorasi data di Amazon Athena memungkinkan Anda menganalisis data yang dikumpulkan dari semua server lokal yang ditemukan oleh Discovery Agent di satu tempat. Setelah Eksplorasi data di Amazon Athena diaktifkan dari konsol Migration Hub (atau dengan menggunakan StartContinousExport API) dan pengumpulan data untuk agen diaktifkan, data yang dikumpulkan oleh agen secara otomatis akan disimpan di bucket S3 Anda secara berkala. Untuk informasi selengkapnya, lihat Menjelajahi data di Amazon Athena.

Eksplorasi data di Amazon Athena memungkinkan Anda menganalisis data yang dikumpulkan dari semua server lokal yang ditemukan oleh Agen Penemuan di satu tempat. Setelah eksplorasi data di Amazon Athena diaktifkan dari konsol Migration Hub (atau dengan menggunakan StartContinousExport API) dan pengumpulan data untuk agen diaktifkan, data yang dikumpulkan oleh agen secara otomatis akan disimpan di bucket S3 Anda secara berkala.

Anda kemudian dapat mengunjungi Amazon Athena untuk menjalankan kueri yang telah ditetapkan untuk menganalisis performa sistem deret waktu untuk setiap server, jenis proses yang berjalan pada setiap server, dan dependensi jaringan antarserver berbeda. Selain itu, Anda dapat menulis kueri kustom Anda sendiri menggunakan Amazon Athena, mengunggah sumber data tambahan yang ada seperti ekspor basis data manajemen konfigurasi (CMDB), dan menghubungkan server yang ditemukan dengan aplikasi bisnis aktual. Anda juga dapat mengintegrasikan database Athena dengan Amazon Quick untuk memvisualisasikan output kueri dan melakukan analisis tambahan.

Topik di bagian ini menjelaskan cara Anda dapat bekerja dengan data Anda di Athena untuk menilai dan merencanakan migrasi lingkungan lokal Anda. AWS

Mengaktifkan eksplorasi data di Amazon Athena

Eksplorasi data di Amazon Athena diaktifkan dengan mengaktifkan Ekspor Berkelanjutan menggunakan konsol Migration Hub atau panggilan API dari. AWS CLI Anda harus mengaktifkan eksplorasi data sebelum dapat melihat dan mulai menjelajahi data yang Anda temukan di Amazon Athena.

Saat Anda mengaktifkan Ekspor Berkelanjutan, peran terkait layanan `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` secara otomatis

digunakan oleh akun Anda. Untuk informasi selengkapnya tentang peran terkait layanan, lihat Izin peran terkait layanan untuk Application Discovery Service.

Petunjuk berikut menunjukkan cara mengaktifkan eksplorasi data di Amazon Athena dengan menggunakan konsol dan. AWS CLI

Turn on with the console

Eksplorasi data di Amazon Athena diaktifkan oleh Ekspor Berkelanjutan diaktifkan secara implisit saat Anda memilih “Mulai pengumpulan data”, atau klik tombol berlabel, “Eksplorasi data di Amazon Athena” di halaman Pengumpul Data di konsol Hub Migrasi.

Untuk mengaktifkan eksplorasi data di Amazon Athena dari konsol

1. Di panel navigasi, pilih Pengumpul Data.
2. Pilih tab Agen.
3. Pilih Mulai pengumpulan data, atau jika Anda sudah mengaktifkan pengumpulan data, klik toggle Eksplorasi data di Amazon Athena.
4. Pada kotak dialog yang dihasilkan dari langkah sebelumnya, klik kotak centang untuk menyetujui biaya terkait dan pilih Lanjutkan atau Aktifkan.

> **Note**
>
> Agen Anda sekarang berjalan dalam mode “ekspor berkelanjutan” yang akan memungkinkan Anda untuk melihat dan bekerja dengan data yang Anda temukan di Amazon Athena. Saat mengaktifkannya untuk pertama kali, mungkin diperlukan waktu 30 menit hingga data Anda muncul di Amazon Athena.

Enable with the AWS CLI

Eksplorasi data di Amazon Athena diaktifkan oleh Ekspor Berkelanjutan yang secara eksplisit diaktifkan melalui panggilan API dari file. AWS CLI Untuk melakukan ini, pertama-tama AWS CLI harus dipasang di lingkungan Anda.

Untuk menginstal AWS CLI dan mengaktifkan eksplorasi data di Amazon Athena

1. Instal AWS CLI untuk sistem operasi Anda (Linux, macOS, atau Windows). Lihat Panduan Pengguna AWS Command Line Interface untuk instruksi.

2. Buka Prompt perintah (Windows) atau Terminal (Linux atau macOS).

   a. Ketik `aws configure` dan tekan Enter.

   b. Masukkan ID Kunci AWS Akses dan Kunci Akses AWS Rahasia Anda.

   c. Masukkan `us-west-2` untuk Nama Wilayah Default.

   d. Masukkan `text` untuk Format Output Default.

3. Ketik perintah berikut ini:

```
aws discovery start-continuous-export
```

> **Note**
>
> Agen Anda sekarang berjalan dalam mode “ekspor berkelanjutan” yang akan memungkinkan Anda untuk melihat dan bekerja dengan data yang Anda temukan di Amazon Athena. Saat mengaktifkannya untuk pertama kali, mungkin diperlukan waktu 30 menit hingga data Anda muncul di Amazon Athena.

Menjelajahi data langsung di Amazon Athena

Setelah Anda mengaktifkan eksplorasi data di Amazon Athena, Anda dapat mulai menjelajahi dan bekerja dengan data terkini terperinci yang ditemukan oleh agen Anda dengan menanyakan data langsung di Athena. Anda dapat menggunakan data untuk membuat spreadsheet, menjalankan analisis biaya, memindahkan kueri ke program visualisasi untuk membuat diagram dependensi jaringan, dan banyak lagi.

Petunjuk berikut menjelaskan cara menjelajahi data agen Anda secara langsung di konsol Athena. Jika Anda tidak memiliki data apa pun di Athena atau belum mengaktifkan eksplorasi data di Amazon Athena, Anda akan diminta oleh kotak dialog untuk mengaktifkan eksplorasi data di Amazon Athena, seperti yang dijelaskan di. Mengaktifkan eksplorasi data di Amazon Athena

Untuk menjelajahi data yang ditemukan agen secara langsung di Athena

1. Di AWS Migration Hub konsol, pilih Server di panel navigasi.
2. Untuk membuka konsol Amazon Athena, pilih Jelajahi data di Amazon Athena.

3. Pada halaman Editor Kueri, di panel navigasi di bawah Basis Data, pastikan bahwa application_discovery_service_database dipilih.

> **Note**
>
> Pada bagian Tabel, tabel-tabel berikut mewakili set data yang dikelompokkan oleh agen.
>
> - os_info_agen
> - network_interface_agent
> - sys_performance_agent
> - processes_agent
> - inbound_connection_agent
> - outbound_connection_agent
> - id_mapping_agent

4. Minta data di konsol Amazon Athena dengan menulis dan menjalankan kueri SQL di Editor Kueri Athena. Sebagai contoh, Anda dapat menggunakan kueri berikut untuk melihat semua alamat IP server yang ditemukan.

```
SELECT * FROM network_interface_agent;
```

Untuk contoh kueri lainnya, lihat Menggunakan kueri yang telah ditentukan di Amazon Athena.

Memvisualisasikan data Amazon Athena

Untuk memvisualisasikan data Anda, kueri dapat di-porting ke program visualisasi seperti Amazon Quick atau alat visualisasi sumber terbuka lainnya seperti Cytoscape, yEd, atau Gelphi. Gunakan alat ini untuk membuat diagram jaringan, bagan ringkasan, dan representasi grafis lainnya. Ketika metode ini digunakan, Anda terhubung ke Athena melalui program visualisasi sehingga dapat mengakses data yang dikumpulkan sebagai sumber untuk menghasilkan visualisasi.

Untuk memvisualisasikan data Amazon Athena Anda menggunakan Quick

1. Masuk ke Amazon Quick.
2. Pilih Hubungkan ke sumber data lain atau unggah file.
3. Pilih Athena. Kotak dialog Sumber data Athena baru akan muncul.

4. Masukkan nama di bidang Nama sumber data.
5. Pilih Buat sumber data.
6. Pilih gents-servers-os tabel A di kotak dialog Pilih tabel Anda dan pilih Pilih.
7. Pada kotak dialog Selesaikan pembuatan set data, pilih Impor ke SPICE untuk analisis yang lebih cepat, dan pilih Visualisasikan.

   Visualisasi Anda dihasilkan.

Menggunakan kueri yang telah ditentukan di Amazon Athena

Bagian ini berisi serangkaian kueri yang telah ditetapkan untuk menjalankan kasus penggunaan umum, seperti analisis TCO dan visualisasi jaringan. Anda dapat menggunakan kueri ini sebagaimana adanya atau mengubahnya sesuai kebutuhan Anda.

Untuk menggunakan kueri yang sudah ditetapkan

1. Di AWS Migration Hub konsol, pilih Server di panel navigasi.
2. Untuk membuka konsol Amazon Athena, pilih Jelajahi data di Amazon Athena.
3. Pada halaman Editor Kueri, di panel navigasi di bawah Basis Data, pastikan bahwa application_discovery_service_database dipilih.
4. Pilih tanda plus (+) pada Editor Kueri untuk membuat tab untuk kueri baru.
5. Salin salah satu kueri dari Kueri yang ditentukan sebelumnya.
6. Tempel kueri ke panel kueri pada tab kueri baru yang baru saja Anda buat.
7. Pilih Jalankan Kueri.

Kueri yang ditentukan sebelumnya

Pilih judul untuk melihat informasi tentang kueri.

Dapatkan alamat IP dan nama host untuk server

Fungsi pembantu tampilan ini mengambil alamat IP dan nama host untuk server tertentu. Anda dapat menggunakan tampilan ini dalam kueri lain. Untuk informasi tentang cara membuat tampilan, lihat BUAT TAMPILAN dalam Panduan Pengguna Amazon Athena.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
```

```
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identifikasi server dengan atau tanpa agen

Query ini dapat membantu Anda melakukan validasi data. Jika Anda telah men-deploy agen di sejumlah server di jaringan Anda, Anda dapat menggunakan kueri ini untuk mengetahui apakah ada server lain di jaringan Anda tanpa agen yang di-deploy pada server tersebut. Dalam kueri ini, kita melihat lalu lintas jaringan inbound dan outbound, dan memfilter lalu lintas untuk alamat IP privat saja. Yakni, alamat IP yang diawali dengan 192, 10, atau 172.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM outbound_connection_agent
WHERE ((("destination_ip" LIKE '192.%')
        OR ("destination_ip" LIKE '10.%'))
        OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
```

```
        FROM network_interface_agent
        WHERE ("ip_address" = "source_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM inbound_connection_agent
WHERE ((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
        OR ("source_ip" LIKE '172.%'));
```

Menganalisis data kinerja sistem untuk server dengan agen

Anda dapat menggunakan kueri ini untuk menganalisis performa sistem dan data pola penggunaan untuk server on-premise Anda yang memiliki agen terinstal pada server tersebut. Kueri ini menggabungkan tabel `system_performance_agent` dengan tabel `os_info_agent` untuk mengidentifikasi nama host untuk setiap server. Kueri ini menghasilkan data penggunaan deret waktu (dengan interval 15 menit) untuk semua server di mana agen berjalan.

```
SELECT "OS"."os_name" "OS Name" ,
    "OS"."os_version" "OS Version" ,
    "OS"."host_name" "Host Name" ,
     "SP"."agent_id" ,
     "SP"."total_num_cores" "Number of Cores" ,
     "SP"."total_num_cpus" "Number of CPU" ,
     "SP"."total_cpu_usage_pct" "CPU Percentage" ,
     "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
     "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
     ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
 Storage" ,
     "SP"."total_ram_in_mb" "Total RAM (MB)" ,
     ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
     "SP"."free_ram_in_mb" "Free RAM (MB)" ,
     "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
     "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
     "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
     "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

Lacak komunikasi keluar antar server berdasarkan nomor port dan detail proses

Kueri ini mendapatkan detail lalu lintas outbound untuk setiap layanan, beserta nomor port dan detail prosesnya.

Sebelum menjalankan kueri, jika Anda belum melakukannya, Anda harus membuat tabel `iana_service_ports_import` yang berisi basis data registri port IANA yang diunduh dari IANA. Untuk informasi tentang cara membuat tabel ini, lihat Membuat tabel impor registri port IANA.

Setelah tabel `iana_service_ports_import` dibuat, buat dua fungsi pembantu tampilan untuk melacak lalu lintas outbound. Untuk informasi tentang cara membuat tampilan, lihat BUAT TAMPILAN dalam Panduan Pengguna Amazon Athena.

Untuk membuat fungsi pembantu pelacakan outbound

1. Buka konsol Athena di https://console.aws.amazon.com/athena/.
2. Buat tampilan `valid_outbound_ips_helper`, menggunakan fungsi pembantu berikut yang mencantumkan semua alamat IP tujuan outbound.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. Buat tampilan `outbound_query_helper`, menggunakan fungsi pembantu berikut yang menentukan frekuensi komunikasi untuk lalu lintas outbound.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("destination_ip" IN
    (SELECT *
    FROM valid_outbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. Setelah Anda membuat tabel `iana_service_ports_import` dan kedua fungsi pembantu tersebut, Anda dapat menjalankan kueri berikut untuk mendapatkan detail tentang lalu lintas outbound untuk setiap layanan, beserta nomor port dan detail prosesnya.

```
SELECT hip1.host_name "Source Host Name",
```

```
        outbound_connections_results0.source_ip "Source IP Address",
        hip2.host_name "Destination Host Name",
        outbound_connections_results0.destination_ip "Destination IP Address",
        outbound_connections_results0.frequency "Connection Frequency",
        outbound_connections_results0.destination_port "Destination Communication
 Port",
        outbound_connections_results0.servicename "Process Service Name",
        outbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT o.source_ip,
         o.destination_ip,
         o.frequency,
         o.destination_port,
         ianap.servicename,
         ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address
```

Lacak komunikasi masuk antar server berdasarkan nomor port dan detail proses

Kueri ini mendapatkan informasi lalu lintas inbound untuk setiap layanan, beserta nomor port dan detail prosesnya.

Sebelum menjalankan kueri ini, jika Anda belum melakukannya, Anda harus membuat tabel `iana_service_ports_import` yang berisi basis data registri port IANA yang diunduh dari IANA. Untuk informasi tentang cara membuat tabel ini, lihat Membuat tabel impor registri port IANA.

Setelah tabel `iana_service_ports_import` dibuat, buat dua fungsi pembantu tampilan untuk melacak lalu lintas inbound. Untuk informasi tentang cara membuat tampilan, lihat BUAT TAMPILAN dalam Panduan Pengguna Amazon Athena.

Untuk membuat fungsi pembantu pelacakan impor

1. Buka konsol Athena di https://console.aws.amazon.com/athena/.
2. Buat tampilan `valid_inbound_ips_helper`, menggunakan fungsi pembantu berikut yang mencantumkan semua alamat IP sumber inbound.

```
CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;
```

3. Buat tampilan `inbound_query_helper`, menggunakan fungsi pembantu berikut yang menentukan frekuensi komunikasi untuk lalu lintas inbound.

```
CREATE OR REPLACE VIEW inbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("source_ip" IN
    (SELECT *
    FROM valid_inbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. Setelah Anda membuat tabel `iana_service_ports_import` dan kedua fungsi pembantu tersebut, Anda dapat menjalankan kueri berikut untuk mendapatkan detail tentang lalu lintas inbound untuk setiap layanan, beserta nomor port dan detail prosesnya.

```
SELECT hip1.host_name "Source Host Name",
         inbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         inbound_connections_results0.destination_ip "Destination IP Address",
         inbound_connections_results0.frequency "Connection Frequency",
         inbound_connections_results0.destination_port "Destination Communication
 Port",
         inbound_connections_results0.servicename "Process Service Name",
         inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
         i.destination_ip,
         i.frequency,
         i.destination_port,
         ianap.servicename,
         ianap.description
```

```
    FROM inbound_query_helper i, iana_service_ports_import ianap
    WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address
```

Identifikasi perangkat lunak yang berjalan dari nomor port

Kueri ini mengidentifikasi perangkat lunak yang berjalan berdasarkan nomor port.

Sebelum menjalankan kueri ini, jika Anda belum melakukannya, Anda harus membuat tabel `iana_service_ports_import` yang berisi basis data registri port IANA yang diunduh dari IANA. Untuk informasi tentang cara membuat tabel ini, lihat Membuat tabel impor registri port IANA.

Jalankan kueri berikut untuk mengidentifikasi perangkat lunak yang berjalan berdasarkan nomor port.

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                  destination_ip,
                  destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                  host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
```

```
ORDER BY cnt_dest_port DESC;
```

Membuat tabel impor registri port IANA

Beberapa kueri yang telah ditetapkan memerlukan tabel bernama `iana_service_ports_import` berisi informasi yang diunduh dari Internet Assigned Numbers Authority (IANA).

Untuk membuat tabel iana_service_ports_import

1. Unduh file CSV basis data registri port IANA dari Registri Nama Layanan dan Nomor Port Protokol Transport pada iana.org.
2. Unggah file ke Amazon S3. Untuk informasi selengkapnya, lihat Bagaimana Cara Mengunggah File dan Folder ke Bucket S3?.
3. Buat tabel baru di Athena dengan nama `iana_service_ports_import`. Untuk instruksi, lihat Buat Tabel dalam Panduan Pengguna Amazon Athena. Pada contoh berikut, Anda perlu mengganti `my_bucket_name` dengan nama bucket S3 tujuan pengunggahan file CSV pada langkah sebelumnya.

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
         ServiceName STRING,
         PortNumber INT,
         TransportProtocol STRING,
         Description STRING,
         Assignee STRING,
         Contact STRING,
         RegistrationDate STRING,
         ModificationDate STRING,
         Reference STRING,
         ServiceCode STRING,
         UnauthorizedUseReported STRING,
         AssignmentNotes STRING
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = ',',
  'quoteChar' = '"',
  'field.delim' = ','
) LOCATION 's3://my_bucket_name/'
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");
```

Menemukan data dengan konsol AWS Migration Hub

AWS Application Discovery Service (Application Discovery Service) terintegrasi dengan AWS Migration Hub (Migration Hub) dan pelanggan dapat melihat dan mengelola pengumpul data, server, dan aplikasi mereka dalam Migration Hub. Bila Anda menggunakan konsol Application Discovery Service, Anda akan dialihkan ke konsol Migration Hub. Bekerja dengan konsol Migration Hub tidak memerlukan langkah atau pengaturan tambahan dari pihak Anda.

Di bagian ini, Anda dapat menemukan cara mengelola dan memantau Application Discovery Service Agentless Collector (Agentless Collector) dan AWS Application Discovery Agent (Discovery Agent) menggunakan konsol.

Topik

- Melihat data di dasbor AWS Migration Hub konsol
- Memulai dan menghentikan pengumpul data di konsol AWS Migration Hub
- Menyortir pengumpul data di konsol AWS Migration Hub
- Melihat server di AWS Migration Hub konsol
- Menyortir server di AWS Migration Hub konsol
- Menandai server di konsol AWS Migration Hub
- Menggunakan AWS Migration Hub untuk mengekspor data server
- Mengelompokkan server di konsol AWS Migration Hub

Melihat data di dasbor AWS Migration Hub konsol

Untuk melihat dasbor utama, pilih Dasbor dari panel navigasi konsol AWS Migration Hub (Migration Hub). Di dasbor utama Migration Hub, Anda dapat melihat statistik tingkat tinggi tentang server, aplikasi, dan pengumpul data seperti Application Discovery Service Agentless Collector (Agentless Collector) dan AWS Application Discovery Agent (Discovery Agent).

Dasbor utama mengumpulkan data dari dasbor Temukan dan Migrasikan di lokasi pusat. Ini memiliki empat panel status dan informasi dan daftar link untuk akses cepat. Dengan menggunakan panel, Anda dapat melihat status ringkasan aplikasi Anda yang paling baru diperbarui. Anda juga bisa mendapatkan akses cepat ke salah satu aplikasi Anda, mendapatkan gambaran umum aplikasi di kondisi yang berbeda, dan melacak kemajuan migrasi dari waktu ke waktu.

Untuk melihat dasbor utama, pilih Dasbor dari panel navigasi, yang berada di sisi kiri beranda konsol Migration Hub.

Memulai dan menghentikan pengumpul data di konsol AWS Migration Hub

Application Discovery Service Agentless Collector (Agentless Collector) dan AWS Application Discovery Agent (Discovery Agent) adalah alat pengumpulan data yang AWS Application Discovery Service digunakan (Application Discovery Service) untuk membantu Anda menemukan infrastruktur yang ada. Langkah-langkah berikut menjelaskan cara mengunduh dan menyebarkan alat pengumpulan data penemuan ini, Menyebarkan Kolektor Tanpa Agen danAWS Agen Penemuan Aplikasi.

Alat pengumpulan data ini menyimpan datanya di repositori Application Discovery Service, yang memberikan detail tentang setiap server dan proses yang berjalan di dalamnya. Saat salah satu alat ini digunakan, Anda dapat memulai, menghentikan, dan melihat data yang dikumpulkan dari konsol AWS Migration Hub (Migration Hub).

Setelah Agen Penemuan AWS Aplikasi (Agen Penemuan) digunakan, Anda dapat memulai atau menghentikan proses pengumpulan data di halaman Pengumpul Data konsol AWS Migration Hub (Migration Hub).

Untuk memulai atau menghentikan alat pengumpulan data

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Pengumpul data.
3. Pilih tab Agen.
4. Centang kotak alat pengumpulan yang ingin Anda mulai atau hentikan.
5. Pilih Mulai pengumpulan data atau Hentikan pengumpulan data.

Menyortir pengumpul data di konsol AWS Migration Hub

Jika Anda menggunakan banyak pengumpul data, Anda dapat mengurutkan daftar pengumpul yang digunakan yang ditampilkan di halaman Pengumpul Data konsol. Anda mengurutkan daftar dengan menerapkan filter di bilah pencarian. Anda dapat mencari dan memfilter sebagian besar kriteria yang ditentukan dalam daftar Pengumpul Data.

Tabel berikut menunjukkan kriteria pencarian yang dapat Anda gunakan untuk Agen, termasuk operator, nilai, dan definisi nilai.

Kriteria Pencarian	Operator	Nilai: Definisi
ID Agen	==	ID agen apa pun yang dipilih dari daftar yang telah diisi sebelumnya dari mana alat pengumpulan diinstal.
Nama host	== !=	Untuk agen, setiap nama host yang dipilih dari daftar host yang telah diisi sebelumnya tempat agen diinstal.
Status pengumpulan	== !=	Dimulai: Data sedang dikumpulkan dan dikirim ke Application Discovery Service Mulai dijadwalkan: Pengumpulan data dijadwalkan untuk dimulai. Data akan dikirim ke Application Discovery Service pada ping berikutnya, dan status akan berubah menjadi Dimulai. Dihentikan: Data tidak dikumpulkan atau dikirim ke Application Discovery Service. Berhenti dijadwalkan: Pengumpulan data dijadwalkan untuk dihentikan. Data akan berhenti dikirimkan ke Application Discovery Service pada ping berikutnya, dan

Kriteria Pencarian	Operator	Nilai: Definisi
		status akan berubah menjadi Dihentikan.
Health	== !=	Sehat: Pengumpulan data tidak diaktifkan. Alat ini berfungsi normal. Tidak sehat: Alat ini dalam keadaan kesalahan. Data tidak dikumpulkan atau dilaporkan. Tidak diketahui: Tidak ada koneksi yang dibuat lebih dari satu jam. Mati: Alat terakhir kali mengomunikasikan “mematikan” karena sistem, layanan, atau daemon dimatikan. Jika terjadi reboot atau peningkatan alat, status akan berubah ke keadaan lain pada siklus pelaporan pertama. Menjalankan: Pengumpulan data diaktifkan. Alat ini berfungsi normal.
Alamat IP	== !=	Alamat IP yang dipilih dari daftar yang telah diisi sebelumnya tempat alat pengumpulan diinstal.

Tabel berikut menunjukkan kriteria pencarian yang dapat Anda gunakan untuk kolektor tanpa agen, termasuk operator, nilai, dan definisi nilai.

Kriteria Pencarian	Operator	Nilai: Definisi
ID	==	Setiap ID kolektor tanpa agen yang dipilih dari daftar yang telah diisi sebelumnya dari mana alat pengumpulan diinstal.
Hostname	== !=	Untuk kolektor tanpa agen, nama host apa pun yang dipilih dari daftar host yang telah diisi sebelumnya di mana kolektor tanpa agen dipasang.
Status	== !=	Mengumpulkan data: Pengumpulan data dihidupkan. Alat ini berfungsi normal. Siap untuk mengkonfigurasi- Pengumpulan data tidak diaktifkan. Alat ini berfungsi normal. Membutuhkan perhatian — Alat ini dalam keadaan kesalahan dan perlu diperhatikan. Tidak diketahui: Tidak ada koneksi yang dibuat lebih dari satu jam. Shut down: Alat terakhir dikomunikasikan “shutting down” karena sistem, layanan, atau daemon dimatikan. Jika terjadi reboot atau peningkatan alat, status akan berubah

Kriteria Pencarian	Operator	Nilai: Definisi
		ke keadaan lain pada siklus pelaporan pertama.
Alamat IP	== !=	Alamat IP yang dipilih dari daftar yang telah diisi sebelumnya tempat alat pengumpulan diinstal.

Untuk menyortir kolektor data dengan menerapkan filter pencarian

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Pengumpul Data.
3. Pilih salah satu kolektor tanpa agen atau tab Agen.
4. Klik di dalam bilah pencarian dan pilih kriteria pencarian dari daftar.
5. Pilih operator dari daftar berikutnya.
6. Pilih nilai dari daftar terakhir.

Melihat server di AWS Migration Hub konsol

Halaman Server menyediakan konfigurasi sistem dan data performa tentang setiap instans server yang dikenal alat pengumpulan data. Anda dapat melihat informasi server, menyortir server dengan filter, menandai server dengan pasangan kunci-nilai, dan mengekspor informasi server dan sistem yang terperinci.

Anda bisa mendapatkan tampilan umum dan tampilan rinci dari server yang ditemukan oleh alat pengumpulan data.

Untuk melihat server yang ditemukan

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Server. Server yang ditemukan muncul dalam daftar server.

3. Untuk detail lebih lanjut tentang server, pilih link server di kolom Info server. Melakukannya menampilkan layar yang menjelaskan server.

Layar detail server menampilkan informasi sistem dan metrik performa. Anda juga dapat menemukan tombol untuk mengekspor dependensi jaringan dan memproses informasi. Untuk mengekspor informasi rinci server, lihat Menggunakan AWS Migration Hub untuk mengekspor data server.

Menyortir server di AWS Migration Hub konsol

Untuk dengan mudah menemukan server tertentu, terapkan filter pencarian untuk memilah-milah semua server ditemukan oleh alat pengumpulan. Anda dapat mencari dan memfilter pada berbagai kriteria.

Untuk menyortir server dengan menerapkan filter pencarian

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Server.
3. Klik di dalam bilah pencarian, dan pilih kriteria pencarian dari daftar.
4. Pilih operator dari daftar berikutnya.
5. Ketik nilai kepekaan huruf besar-kecil untuk kriteria pencarian yang Anda pilih, dan tekan Enter.
6. Beberapa filter dapat diterapkan dengan mengulangi langkah 2 - 4.

Menandai server di konsol AWS Migration Hub

Untuk membantu perencanaan migrasi dan membantu tetap teratur, Anda dapat membuat beberapa tag untuk setiap server. Tag adalah pasangan kunci-nilai yang ditetapkan pengguna yang dapat menyimpan data kustom atau metadata tentang server. Anda dapat menandai server individual atau beberapa server dalam satu operasi. AWS Application Discovery Service (Application Discovery Service) AWS tag mirip dengan tag, tetapi kedua jenis tag tidak dapat digunakan secara bergantian.

Anda dapat menambahkan atau menghapus beberapa tag untuk satu atau beberapa server dari halaman Server utama. Pada halaman detail server, Anda dapat menambahkan atau menghapus satu atau lebih tag untuk server yang dipilih. Anda dapat melakukan semua jenis tugas penandaan yang melibatkan beberapa server atau tag dalam satu operasi. Anda juga dapat menghapus tag.

Untuk menambahkan tag ke satu atau lebih server

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Server.
3. Di kolom Info server, pilih tautan server untuk server yang ingin Anda tambahkan tag. Untuk menambahkan tag ke lebih dari satu server pada satu waktu, klik di dalam kotak centang dari beberapa server.
4. Pilih Tambahkan tag, lalu pilih Tambahkan tag baru.
5. Di kotak dialog, ketikkan kunci di bidang Kunci, dan secara opsional nilai di bidang Nilai.

   Tambahkan lebih banyak tag dengan memilih Tambahkan tag baru dan menambahkan lebih banyak informasi.
6. Pilih Simpan.

Untuk menghapus tag dari satu atau lebih server

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Server.
3. Di kolom Info server, pilih link server untuk server yang ingin Anda hapus tagnya. Pilih kotak centang beberapa server untuk menghapus tag dari lebih dari satu server sekaligus.
4. Pilih Hapus tag.
5. Pilih setiap tag yang ingin Anda hapus.
6. Pilih Konfirmasi.

Menggunakan AWS Migration Hub untuk mengekspor data server

Topik ini menjelaskan cara mengekspor data server dengan menggunakan Konsol Manajemen AWS, the AWS Command Line Interface, atau API.

Untuk menggunakan data Konsol Manajemen AWS untuk mengekspor server untuk semua server

1. Masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.

2. Di panel navigasi kiri di bawah Temukan, pilih Server.
3. Pilih Tindakan, lalu pilih Ekspor data penemuan.
4. Di bagian Ekspor di bagian bawah layar, pilih Ekspor detail server. Tindakan ini menghasilkan file.zip yang menyertakan file.csv yang dijelaskan dalam tabel berikut.

Nama file	Deskripsi
{account_id} _Application.csv	Detail setiap aplikasi, termasuk jumlah server, nama, dan deskripsi.
{account_id} _ .csv ApplicationResourc eAssociation	Hubungan antara server dan aplikasi.
{account_id} _ ImportTemplate	Ringkasan aplikasi dan tag masing-masing server. File ini dapat dimodifikasi dan diimpor ulang untuk memperbarui aplikasi yang terkait dengan server.
{account_id} _ .csv NetworkInterface	Rincian setiap antarmuka jaringan termasuk server terkait, alamat, dan sakelar.
{account_id} _Server.csv	Rincian setiap server, termasuk sistem operasi, nama host, dan hypervisor.
{account_id} _ .csv SystemPerformance	Rincian setiap server, termasuk CPU, konfigurasi memori dan penyimpanan, dan kinerja.
{account_id} _Tags.csv	Detail setiap tag yang terkait dengan server.
{account_id} _ Info.csv VMware	Detail setiap VMware konfigurasi, termasuk MoreF, VMName, dan vCenter.

Untuk menggunakan data agen ekspor untuk server tertentu Konsol Manajemen AWS

1. Masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi kiri di bawah Temukan, pilih Server.

3. Tempatkan kursor di bidang pencarian di bawah Server. Daftar drop-down muncul. Dalam daftar itu, di bawah Properties, pilih Source, lalu pilih operator =, lalu pilih Source = Agent.
4. Dalam hasil pencarian, pilih nama server yang ingin Anda ekspor datanya. Tindakan ini membawa Anda ke halaman detail untuk server itu.
5. Masukkan waktu mulai dan waktu berakhir, lalu pilih Ekspor. File zip yang diekspor menyertakan file.csv yang dijelaskan dalam tabel berikut.

{account_id} _ .csv destinationProcess Connection	Detail koneksi masuk ke server.
{account_id} _networkInterface.csv	Detail setiap antarmuka jaringan termasuk alamat, topeng, dan nama
{account_id} _osInfo.csv	Rincian sistem operasi termasuk tipe CPU, hypervisor dan nama sistem operasi.
{account_id} _process.csv	Detail proses yang berjalan di server.
{account_id} _ .csv sourceProcessConne ction	Detail koneksi keluar yang berasal dari server.
{account_id} _systemPerformance.csv	Rincian CPU, memori dan konfigurasi penyimpanan & kinerja untuk server.

Untuk menggunakan AWS Command Line Interface atau API untuk mengekspor data server

1. Jalankan start-export-task. Operasi API yang sesuai adalah StartExportTask
2. Jalankan describe-export-tasks. Operasi API yang sesuai adalah DescribeExportTasks.

Mengelompokkan server di konsol AWS Migration Hub

Beberapa server yang Anda temukan mungkin perlu dimigrasi bersama agar tetap berfungsi. Dalam kasus ini, Anda dapat secara logis menentukan dan mengelompokkan server yang ditemukan ke dalam aplikasi.

Sebagai bagian dari proses pengelompokan, Anda dapat mencari, memfilter, dan menambahkan tag.

Untuk mengelompokkan server ke aplikasi baru atau yang sudah ada

1. Menggunakan AWS akun Anda, masuk ke Konsol Manajemen AWS dan buka konsol Migration Hub di https://console.aws.amazon.com/migrationhub/.
2. Di panel navigasi konsol Migration Hub di bawah Temukan, pilih Server.
3. Dalam daftar server, pilih setiap server yang ingin Anda kelompokkan ke aplikasi baru atau yang sudah ada.

   Untuk membantu memilih server untuk grup Anda, Anda dapat mencari dan memfilter kriteria yang Anda tentukan dalam daftar server. Klik di dalam bilah pencarian dan pilih item dari daftar, pilih operator dari daftar berikutnya, lalu ketik kriteria Anda.
4. Opsional: Untuk setiap server yang dipilih, pilih Tambahkan tag, ketik nilai untuk Kunci, dan Anda dapat mengetik nilai untuk Nilai.
5. Pilih Kelompokkan sebagai aplikasi untuk membuat aplikasi, atau menambahkan ke aplikasi yang sudah ada.
6. Di kotak dialog Kelompokkan sebagai aplikasi, pilih Kelompokkan sebagai aplikasi baru atau Tambahkan ke aplikasi yang sudah ada.

   a. Jika Anda memilih Kelompokkan sebagai aplikasi baru, ketik nama untuk Nama aplikasi. Secara opsional, Anda dapat mengetikkan deskripsi untuk Deskripsi aplikasi.

   b. Jika Anda memilih Tambahkan ke aplikasi yang sudah ada, pilih nama aplikasi tempat Anda menambahkan dalam daftar.
7. Pilih Simpan.

Menggunakan Application Discovery Service API untuk menanyakan item konfigurasi yang ditemukan

Item konfigurasi adalah aset TI yang ditemukan di pusat data Anda oleh agen atau oleh impor. Saat Anda menggunakan AWS Application Discovery Service (Application Discovery Service), Anda menggunakan API untuk menentukan filter dan menanyakan item konfigurasi tertentu untuk aset server, aplikasi, proses, dan koneksi. Untuk informasi tentang API, lihat Referensi API Application Discovery Service.

Tabel di bagian berikut mencantumkan filter input dan opsi penyortiran output yang tersedia untuk dua tindakan Application Discovery Service:

- `DescribeConfigurations`
- `ListConfigurations`

Opsi pemfilteran dan penyortiran diatur berdasarkan jenis aset yang diterapkan (server, aplikasi, proses, atau koneksi).

> **Important**
>
> Hasil yang dikembalikan oleh `DescribeConfigurationsListConfigurations`,, dan `StartExportTask` mungkin tidak berisi pembaruan terbaru. Untuk informasi selengkapnya, lihat the section called “Konsistensi akhirnya”.

Menggunakan **`DescribeConfigurations`** tindakan

`DescribeConfigurations`Tindakan mengambil atribut untuk daftar konfigurasi IDs. Semua yang disediakan IDs harus untuk jenis aset yang sama (server, aplikasi, proses, atau koneksi). Bidang output khusus untuk jenis aset yang dipilih. Sebagai contoh, output untuk item konfigurasi server menyertakan daftar atribut tentang server, seperti nama host, sistem operasi, dan jumlah kartu jaringan. Untuk informasi selengkapnya tentang sintaks perintah, lihat DescribeConfigurations.

`DescribeConfigurations`Tindakan ini tidak mendukung penyaringan.

Bidang output untuk **`DescribeConfigurations`**

Tabel berikut, yang diatur berdasarkan jenis aset, mencantumkan bidang output tindakan`DescribeConfigurations` yang didukung. Yang ditandai sebagai wajib selalu ada dalam output.

Aset server

Bidang	Wajib
`server.agentId`	
`server.applications`	
`server.applications.hasMore Values`	
`server.configurationId`	x
`server.cpuType`	
`server.hostName`	
`server.hypervisor`	
`server.networkInterfaceInfo`	
`server.networkInterfaceInfo .hasMoreValues`	
`server.osName`	
`server.osVersion`	
`server.tags`	
`server.tags.hasMoreValues`	
`server.timeOfCreation`	x
`server.type`	

Bidang	Wajib
server.performance.avgCpuUsagePct	
server.performance.avgDiskReadIOPS	
server.performance.avgDiskReadsPerSecondInKB	
server.performance.avgDiskWriteIOPS	
server.performance.avgDiskWritesPerSecondInKB	
server.performance.avgFreeRAMInKB	
server.performance.avgNetworkReadsPerSecondInKB	
server.performance.avgNetworkWritesPerSecondInKB	
server.performance.maxCpuUsagePct	
server.performance.maxDiskReadIOPS	
server.performance.maxDiskReadsPerSecondInKB	
server.performance.maxDiskWriteIOPS	
server.performance.maxDiskWritesPerSecondInKB	

Bidang	Wajib
server.performance.maxNetwo rkReadsPerSecondInKB	
server.performance.maxNetwo rkWritesPerSecondInKB	
server.performance.minFreeR AMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetwo rkCards	
server.performance.totalRAMInKB	

Memproses aset

Bidang	Wajib
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

Aset aplikasi

Bidang	Wajib
application.configurationId	x
application.description	
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

Menggunakan **ListConfigurations** tindakan

TindakanListConfigurations mengambil daftar item konfigurasi sesuai dengan kriteria yang Anda tentukan dalam filter. Untuk informasi selengkapnya tentang sintaks perintah, lihat ListConfigurations.

Bidang output untuk **ListConfigurations**

Tabel berikut, yang diatur berdasarkan jenis aset, mencantumkan bidang output tindakanListConfigurations yang didukung. Yang ditandai sebagai wajib selalu ada dalam output.

Aset server

Bidang	Wajib
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	

Bidang	Wajib
server.timeOfCreation	x
server.type	

Memproses aset

Bidang	Wajib
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x
server.agentId	
server.configurationId	x

Aset aplikasi

Bidang	Wajib
application.configurationId	x
application.description	
application.name	x
application.serverCount	x
application.timeOfCreation	x
application.lastModifiedTime	x

Aset koneksi

Bidang	Wajib
connection.destinationIp	x
connection.destinationPort	x
connection.ipVersion	x
connection.latestTimestamp	x
connection.occurrence	x
connection.sourceIp	x
connection.transportProtocol	
destinationProcess.configurationId	
destinationProcess.name	
destinationServer.configurationId	
destinationServer.hostName	
sourceProcess.configurationId	
sourceProcess.name	
sourceServer.configurationId	
sourceServer.hostName	

Filter yang didukung untuk **`ListConfigurations`**

Tabel berikut, yang diatur berdasarkan jenis aset, mencantumkan filter yang didukung untuk tindakan`ListConfigurations`. Filter dan nilai berada dalam key/value hubungan yang ditentukan

oleh salah satu kondisi logis yang didukung. Anda dapat mengurutkan output dari filter yang ditunjukkan.

Aset server

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Setiap ID konfigurasi server yang valid	Tidak ada
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.agentId`	• EQUALS	• String	Tidak ada

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
	• NOT_EQUALS • EQ • NE		
`server.connectorId`	• EQUALS • NOT_EQUALS • EQ • NE	• String	Tidak ada
`server.type`	• EQUALS • NOT_EQUALS • EQ • NE	String dengan salah satu nilai berikut: • EC2 • LAINNYA • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	Tidak ada
`server.vmWareInfo.morefId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`server.vmWareInfo.vcenterId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.vmWareInfo.hostId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.networkInterfaceInfo.portGroupId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.networkInterfaceInfo.portGroupName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`server.networkInterfaceInfo.virtualSwitchName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.networkInterfaceInfo.ipAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.networkInterfaceInfo.macAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.performance.avgCpuUsagePct`	• GE • LE • GT • LT	• Persentase	Tidak ada
`server.performance.totalDiskFreeSizeInKB`	• GE • LE • GT • LT	• Ganda	Tidak ada

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`server.performance.avgFreeRAMInKB`	• GE • LE • GT • LT	• Ganda	Tidak ada
`server.tag.value`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.tag.key`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`server.application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Setiap ID konfigurasi aplikasi yang valid	Tidak ada
`server.process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	Tidak ada
`server.process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada
`server.process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Tidak ada

Aset aplikasi

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ApplicationId	Tidak ada
`application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.serverCount`	Pemfilteran tidak didukung.	Pemfilteran tidak didukung.	• ASC • DESC
`application.timeOfCreation`	Pemfilteran tidak didukung.	Pemfilteran tidak didukung.	• ASC • DESC

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`application.lastModifiedTime`	Pemfilteran tidak didukung.	Pemfilteran tidak didukung.	• ASC • DESC
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	Tidak ada

Memproses aset

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE	• String	• ASC • DESC

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
	• CONTAINS • NOT_CONTAINS		
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`server.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	

Aset koneksi

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`connection.sourceIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationPort`	• EQUALS • NOT_EQUALS • EQ • NE	• Bilangan Bulat	• ASC • DESC

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`sourceServer.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`sourceServer.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`destinationServer.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	
`sourceProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`sourceProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`sourceProcess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

Filter	Kondisi yang didukung	Nilai yang didukung	Penyortiran yang didukung
`destinationProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Konsistensi akhirnya di API AWS Application Discovery Service

Operasi pembaruan berikut pada akhirnya konsisten. Pembaruan mungkin tidak langsung terlihat oleh operasi baca StartExportTask, DescribeConfigurations, dan ListConfigurations.

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- UpdateApplication

Saran untuk mengelola konsistensi akhirnya:

- Saat Anda menjalankan operasi baca StartExportTask, DescribeConfigurations, atau ListConfigurations(atau AWS CLI perintah yang sesuai), gunakan algoritma backoff eksponensial untuk memberikan waktu yang cukup bagi operasi pembaruan sebelumnya untuk menyebar melalui sistem. Untuk melakukan ini, jalankan operasi baca berulang kali, dimulai dengan waktu tunggu dua detik, dan tingkatkan secara bertahap hingga lima menit waktu tunggu.
- Tambahkan waktu tunggu antara operasi berikutnya, bahkan jika operasi pembaruan mengembalikan respons 200 - OK. Terapkan algoritma backoff eksponensial dimulai dengan beberapa detik waktu tunggu, dan tingkatkan secara bertahap hingga sekitar lima menit waktu tunggu.

Akses AWS Application Discovery Service menggunakan endpoint antarmuka ()AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan. AWS Application Discovery Service Anda dapat mengakses Application Discovery Service seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses Application Discovery Service.

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, yang didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola oleh permintaan yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan untuk Application Discovery Service.

Untuk informasi selengkapnya, lihat Mengakses Layanan AWS melalui AWS PrivateLink di Panduan AWS PrivateLink .

Pertimbangan untuk Application Discovery Service

Sebelum Anda menyiapkan titik akhir antarmuka untuk Application Discovery Service, tinjau Akses AWS layanan menggunakan titik akhir VPC antarmuka di Panduan.AWS PrivateLink

Application Discovery Service mendukung dua antarmuka: Satu untuk melakukan panggilan ke semua tindakan API-nya, dan yang kedua untuk Agentless Collector dan AWS Application Discovery Agent untuk mengirim data penemuan.

Membuat sebuah titik akhir antarmuka

Anda dapat membuat titik akhir antarmuka menggunakan konsol VPC Amazon atau () AWS Command Line Interface .AWS CLIUntuk informasi selengkapnya, lihat Mengakses AWS layanan menggunakan titik akhir VPC antarmuka di Panduan.AWS PrivateLink

For Application Discovery Service

Buat endpoint antarmuka untuk Application Discovery Service menggunakan nama layanan berikut:

```
com.amazonaws.region.discovery
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API ke Application Discovery Service menggunakan nama DNS Regional default. Misalnya, `discovery.us-east-1.amazonaws.com`.

For Agentless Collector and AWS Application Discovery Agent

Buat endpoint antarmuka menggunakan nama layanan berikut:

```
com.amazonaws.region.arsenal-discovery
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API ke Application Discovery Arsenal menggunakan nama DNS Regional default. Misalnya, `arsenal-discovery.us-east-1.amazonaws.com`.

Buat kebijakan titik akhir untuk titik akhir antarmuka Anda

Kebijakan endpoint adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir antarmuka. Kebijakan endpoint default memungkinkan akses penuh ke AWS layanan melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan ke AWS layanan dari VPC Anda, lampirkan kebijakan titik akhir kustom ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM).
- Tindakan yang dapat dilakukan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh: kebijakan titik akhir VPC

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke tindakan yang tercantum untuk semua prinsip di semua sumber daya.

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

Menggunakan titik akhir VPC untuk Agentless Collector dan Application Discovery Agent AWS

Agentless Collector dan AWS Application Discovery Agent tidak mendukung endpoint yang dapat dikonfigurasi. Sebagai gantinya, gunakan fitur DNS pribadi untuk titik akhir VPC `arsenal-discovery` Amazon.

- Siapkan tabel Direct Connect rute untuk merutekan alamat IP AWS pribadi ke VPC. Misalnya, tujuan = 10.0.0.0/8 dan target = lokal. Untuk pengaturan ini, Anda memerlukan setidaknya perutean untuk alamat IP pribadi titik akhir VPC `arsenal-discovery` Amazon ke VPC.
- Gunakan fitur DNS pribadi titik akhir VPC `arsenal-discovery` Amazon karena Agentless Collector tidak mendukung titik akhir Arsenal yang dapat dikonfigurasi.
- Siapkan titik akhir VPC `arsenal-discovery` Amazon di subnet pribadi dengan VPC yang sama dengan tempat Anda merutekan lalu lintas. Direct Connect
- Siapkan titik akhir VPC `arsenal-discovery` Amazon dengan grup keamanan yang memungkinkan lalu lintas masuk dari dalam VPC (misalnya, 10.0.0.0/8).
- Siapkan resolver masuk Amazon Route 53 untuk merutekan resolusi DNS untuk nama DNS pribadi titik akhir `arsenal-discovery` VPC Amazon, yang akan menyelesaikan ke IP pribadi titik akhir VPC. Jika Anda tidak melakukannya, kolektor akan melakukan resolusi DNS dengan menggunakan resolver lokal dan akan menggunakan endpoint Arsenal publik, dan lalu lintas tidak akan melalui VPC.
- Jika Anda menonaktifkan semua lalu lintas publik, fitur pembaruan otomatis akan gagal. Itu karena Kolektor Tanpa Agen mengambil pembaruan dengan mengirimkan permintaan ke titik akhir Amazon ECR. Agar fitur pembaruan otomatis berfungsi tanpa mengirim permintaan melalui internet publik, siapkan titik akhir VPC untuk layanan Amazon ECR dan aktifkan fitur DNS pribadi untuk titik akhir ini.

Keamanan di AWS Application Discovery Service

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain termasuk sensitivitas data, kebutuhan organisasi, serta undang-undang dan peraturan yang berlaku.

Untuk menggunakan Agen Penemuan AWS Aplikasi atau Application Discovery Service Agentless Collector, Anda harus memberikan kunci akses ke akun Anda AWS . Informasi ini kemudian disimpan di infrastruktur lokal Anda. Sebagai bagian dari model tanggung jawab bersama, Anda bertanggung jawab untuk mengamankan akses ke infrastruktur Anda.

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

Topik

- Identity and Access Management untuk AWS Application Discovery Service
- Logging panggilan Application Discovery Service API dengan AWS CloudTrail

Identity and Access Management untuk AWS Application Discovery Service

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengendalikan siapa yang dapat terautentikasi (masuk) dan berwenang (memiliki izin) untuk menggunakan sumber daya Application Discovery Service. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Application Discovery Service bekerja dengan IAM
- AWS kebijakan terkelola untuk AWS Application Discovery Service
- AWS Application Discovery Service contoh kebijakan berbasis identitas
- Menggunakan peran terkait layanan untuk Application Discovery Service
- Pemecahan Masalah AWS Application Discovery Service Identitas dan Akses

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan Masalah AWS Application Discovery Service Identitas dan Akses)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana AWS Application Discovery Service bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat AWS Application Discovery Service contoh kebijakan berbasis identitas)

Mengautentikasi dengan identitas

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

Anda dapat masuk sebagai identitas federasi menggunakan kredensil dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan

memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola 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. Contohnya termasuk 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. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

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 (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs
Untuk mempelajari selengkapnya ACLs, lihat Ringkasan daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. 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 AWS Application Discovery Service bekerja dengan IAM

Sebelum menggunakan IAM untuk mengelola akses ke Application Discovery Service, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan dengan Application Discovery Service. Untuk mendapatkan tampilan tingkat tinggi tentang cara Application Discovery Service dan AWS layanan lainnya bekerja dengan IAM, lihat AWS Layanan yang Bekerja dengan IAM di Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas Application Discovery Service
- Kebijakan berbasis sumber daya Application Discovery Service
- Otorisasi berdasarkan tag Application Discovery Service
- Peran IAM Application Discovery Service

Kebijakan berbasis identitas Application Discovery Service

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. Application Discovery Service mendukung tindakan, sumber daya, dan kunci syarat tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi Elemen Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan dalam Application Discovery Service menggunakan prefiks berikut sebelum tindakan: `discovery:`. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Application Discovery Service menentukan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

```
"Action": "discovery:Describe*"
```

Untuk melihat daftar tindakan Application Discovery Service, lihat Tindakan yang Ditetapkan oleh AWS Application Discovery Service dalam Panduan Pengguna IAM.

Sumber daya

Application Discovery Service tidak mendukung penetapan sumber daya ARNs dalam kebijakan. Untuk memisahkan akses, buat dan gunakan terpisah Akun AWS.

Kunci syarat

Application Discovery Service tidak menyediakan kunci syarat khusus layanan, tetapi mendukung penggunaan beberapa kunci syarat global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Application Discovery Service, lihat AWS Application Discovery Service contoh kebijakan berbasis identitas.

Kebijakan berbasis sumber daya Application Discovery Service

Application Discovery Service tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tag Application Discovery Service

Application Discovery Service tidak mendukung penandaan sumber daya atau pengendalian akses berdasarkan tag.

Peran IAM Application Discovery Service

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensil sementara dengan Application Discovery Service

Application Discovery Service tidak mendukung penggunaan kredensial sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Application Discovery Service mendukung peran terkait layanan. Untuk detail tentang membuat atau mengelola peran terkait layanan Application Discovery Service, lihat Menggunakan peran terkait layanan untuk Application Discovery Service.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Application Discovery Service mendukung peran layanan.

AWS kebijakan terkelola untuk AWS Application Discovery Service

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 yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang 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: AWSApplication DiscoveryServiceFullAccess

`AWSApplicationDiscoveryServiceFullAccess`Kebijakan ini memberikan akses akun pengguna IAM ke Application Discovery Service dan Migration Hub. APIs

Akun pengguna IAM dengan kebijakan terlampir ini dapat mengonfigurasi Application Discovery Service, memulai dan menghentikan agen, memulai dan menghentikan penemuan tanpa agen, dan kueri data dari database AWS Discovery Service. Untuk contoh kebijakan ini, lihat Memberikan akses penuh ke Application Discovery Service.

AWS kebijakan terkelola: AWSApplication DiscoveryAgentlessCollectorAccess

Kebijakan `AWSApplicationDiscoveryAgentlessCollectorAccess` terkelola memberikan akses kepada Application Discovery Service Agentless Collector (Agentless Collector) untuk mendaftar dan berkomunikasi dengan Application Discovery Service, dan berkomunikasi dengan layanan lain. AWS

Kebijakan ini harus dilampirkan ke pengguna IAM yang kredensialnya digunakan untuk mengonfigurasi Kolektor Tanpa Agen.

Detail izin

Kebijakan ini mencakup izin berikut.

- `arsenal`— Memungkinkan kolektor untuk mendaftar dengan aplikasi Application Discovery Service. Ini diperlukan untuk dapat mengirim data yang dikumpulkan kembali ke AWS.
- `ecr-public`— Memungkinkan kolektor untuk melakukan panggilan ke Amazon Elastic Container Registry Public (Amazon ECR Public) di mana pembaruan terbaru ditemukan untuk kolektor.
- `mgh`— Memungkinkan kolektor AWS Migration Hub untuk menelepon untuk mengambil wilayah asal akun yang digunakan untuk mengkonfigurasi kolektor. Ini diperlukan untuk mengetahui wilayah mana data yang dikumpulkan harus dikirim.
- `sts`— Memungkinkan kolektor untuk mengambil token pembawa layanan sehingga kolektor dapat melakukan panggilan ke Amazon ECR Public untuk mendapatkan pembaruan terbaru.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:DescribeImages"
            ],
            "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ecr-public:GetAuthorizationToken"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "mgh:GetHomeRegion"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:GetServiceBearerToken"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSApplication DiscoveryAgentAccess

Kebijakan `AWSApplicationDiscoveryAgentAccess` memberikan akses bagi Application Discovery Agent untuk mendaftar dan berkomunikasi dengan Application Discovery Service.

Anda melampirkan kebijakan ini untuk setiap pengguna yang kredensialnya digunakan oleh Application Discovery Agent.

Kebijakan ini juga memberikan akses ke Arsenal bagi pengguna. Arsenal adalah layanan agen yang dikelola dan diselenggarakan oleh AWS. Arsenal meneruskan data ke Application Discovery Service di cloud. Untuk contoh kebijakan ini, lihat Memberikan akses ke agen penemuan.

AWS kebijakan terkelola: AWSAgentless DiscoveryService

`AWSAgentlessDiscoveryService`Kebijakan ini memberikan Konektor Penemuan AWS Tanpa Agen yang berjalan di Server VMware vCenter Anda akses untuk mendaftar, berkomunikasi, dan berbagi metrik kesehatan konektor dengan Application Discovery Service.

Anda melampirkan kebijakan ini untuk setiap pengguna yang kredensialnya digunakan oleh konektor.

AWS kebijakan terkelola: ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Jika akun IAM Anda memiliki `AWSApplicationDiscoveryServiceFullAccess` kebijakan yang dilampirkan, secara otomatis `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` dilampirkan ke akun Anda saat Anda mengaktifkan eksplorasi data di Amazon Athena.

Kebijakan ini AWS Application Discovery Service memungkinkan Anda membuat aliran Amazon Data Firehose untuk mengubah dan mengirimkan data yang dikumpulkan oleh AWS Application Discovery Service agen ke bucket Amazon S3 di akun Anda. AWS

Selain itu, kebijakan ini membuat AWS Glue Data Catalog dengan database baru bernama application_discovery_service_database dan skema tabel untuk memetakan data yang dikumpulkan oleh agen. Untuk contoh kebijakan ini, lihat Memberikan izin untuk pengumpulan data agen.

AWS kebijakan terkelola: AWSDiscovery ContinuousExportFirehosePolicy

`AWSDiscoveryContinuousExportFirehosePolicy`Kebijakan ini diperlukan untuk menggunakan eksplorasi data di Amazon Athena. Ini memungkinkan Amazon Data Firehose untuk menulis data yang dikumpulkan dari Application Discovery Service ke Amazon S3. Untuk informasi selengkapnya tentang kebijakan ini, lihat Menciptakan AWSApplication DiscoveryServiceFirehose peran. Untuk contoh kebijakan ini, lihat Memberikan izin untuk eksplorasi data.

Menciptakan AWSApplication DiscoveryServiceFirehose peran

Administrator melampirkan kebijakan terkelola ke akun pengguna IAM Anda. Saat menggunakan `AWSDiscoveryContinuousExportFirehosePolicy` kebijakan, administrator harus terlebih dahulu membuat peran bernama AWSApplicationDiscoveryServiceFirehoseFirehose sebagai entitas tepercaya dan kemudian melampirkan `AWSDiscoveryContinuousExportFirehosePolicy` kebijakan ke peran, seperti yang ditunjukkan dalam prosedur berikut.

Untuk membuat IAM role AWSApplicationDiscoveryServiceFirehose

1. Di konsol IAM, pilih Peran pada panel panel navigasi.
2. Pilih Buat Peran.
3. Pilih Kinesis.

4. Pilih Kinesis Firehose sebagai kasus penggunaan Anda.
5. Pilih Berikutnya: Izin.
6. Di bawah Kebijakan Filter, cari AWSDiscoveryContinuousExportFirehosePolicy.
7. Pilih kotak di samping AWSDiscoveryContinuousExportFirehosePolicy, lalu pilih Berikutnya: Tinjau.
8. Masukkan AWSApplicationDiscoveryServiceFirehosesebagai nama peran, lalu pilih Buat peran.

Application Discovery Service memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Application Discovery Service sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat Dokumen untuk AWS Application Discovery Service.

Perubahan	Deskripsi	Date
AWSApplicationDiscoveryAgentlessCollectorAccess— Kebijakan baru tersedia dengan peluncuran Agentless Collector	Application Discovery Service menambahkan kebijakan terkelola baru `AWSApplicationDiscoveryAgentlessCollectorAccess` yang memberikan akses kepada Agentless Collector untuk mendaftar dan berkomunikasi dengan Application Discovery Service, dan berkomunikasi dengan layanan lain. AWS	Agustus 16, 2022
Application Discovery Service mulai melacak perubahan	Application Discovery Service mulai melacak perubahan untuk kebijakan yang AWS dikelola.	1 Maret 2021

AWS Application Discovery Service contoh kebijakan berbasis identitas

Secara default, pengguna dan peran IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya Application Discovery Service. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

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

Topik

- Praktik terbaik kebijakan
- Memberikan akses penuh ke Application Discovery Service
- Memberikan akses ke agen penemuan
- Memberikan izin untuk pengumpulan data agen
- Memberikan izin untuk eksplorasi data
- Memberikan izin untuk menggunakan diagram jaringan konsol Migration Hub

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Application Discovery Service 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 Layanan AWS, seperti 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 dengan 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 Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

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

Memberikan akses penuh ke Application Discovery Service

Kebijakan AWSApplication DiscoveryServiceFullAccess terkelola memberikan akses akun pengguna IAM ke Application Discovery Service dan Migration Hub. APIs

Akun pengguna IAM yang dilampiri kebijakan ini dapat mengonfigurasi Application Discovery Service, memulai dan menghentikan agen, memulai dan menghentikan penemuan tanpa agen, dan meminta data dari basis data Layanan Penemuan AWS . Untuk informasi selengkapnya tentang kebijakan ini, lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.

Example AWSApplicationDiscoveryServiceFullAccess kebijakan

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Memberikan akses ke agen penemuan

Kebijakan AWSApplication DiscoveryAgentAccess terkelola memberikan akses kepada Agen Penemuan Aplikasi untuk mendaftar dan berkomunikasi dengan Application Discovery Service. Untuk informasi selengkapnya tentang kebijakan ini, lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.

Lampirkan kebijakan ini untuk setiap pengguna yang kredensialnya digunakan oleh Application Discovery Agent.

Kebijakan ini juga memberikan akses ke Arsenal bagi pengguna. Arsenal adalah layanan agen yang dikelola dan diselenggarakan oleh AWS. Arsenal meneruskan data ke Application Discovery Service di cloud.

Example AWSApplicationDiscoveryAgentAccess Kebijakan

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        }
    ]
}
```

Memberikan izin untuk pengumpulan data agen

Kebijakan ApplicationDiscoveryServiceContinuousExportServiceRolePolicy terkelola AWS Application Discovery Service memungkinkan Anda membuat aliran Amazon Data Firehose untuk mengubah dan mengirimkan data yang dikumpulkan oleh agen Application Discovery Service ke bucket Amazon S3 di akun Anda. AWS

Selain itu, kebijakan ini membuat Katalog AWS Glue Data dengan database baru yang disebut `application_discovery_service_database` dan skema tabel untuk memetakan data yang dikumpulkan oleh agen.

Untuk informasi selengkapnya tentang kebijakan ini, lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

JSON

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

```
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-
discovery-service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
```

```
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-
service/firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

Memberikan izin untuk eksplorasi data

AWSDiscoveryContinuousExportFirehosePolicy Kebijakan ini diperlukan untuk menggunakan eksplorasi data di Amazon Athena. Ini memungkinkan Amazon Data Firehose untuk menulis data yang dikumpulkan dari Application Discovery Service ke Amazon S3. Untuk informasi selengkapnya tentang kebijakan ini, lihat Menciptakan AWSApplication DiscoveryServiceFirehose peran.

Example AWSDiscoveryContinuousExportFirehosePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-application-discovery-service-*",
                "arn:aws:s3:::aws-application-discovery-service-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
            ]
        }
    ]
}
```

Memberikan izin untuk menggunakan diagram jaringan konsol Migration Hub

Untuk memberikan akses ke diagram jaringan AWS Migration Hub konsol saat membuat kebijakan berbasis identitas yang mengizinkan atau menolak akses ke Application Discovery Service atau Migration Hub, Anda mungkin perlu menambahkan `discovery:GetNetworkConnectionGraph` tindakan ke kebijakan.

Anda harus menggunakan `discovery:GetNetworkConnectionGraph` tindakan dalam kebijakan baru atau memperbarui kebijakan lama jika hal berikut berlaku untuk kebijakan tersebut:

- Kebijakan ini mengizinkan atau menolak akses ke Application Discovery Service atau Migration Hub.
- Kebijakan ini memberikan izin akses menggunakan satu tindakan penemuan yang lebih spesifik seperti `discovery:`*`action-name`* bukan. `discovery:*`

Contoh berikut menunjukkan cara menggunakan `discovery:GetNetworkConnectionGraph` tindakan dalam kebijakan IAM.

Example

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["discovery:GetNetworkConnectionGraph"],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi tentang diagram jaringan Hub Migrasi, lihat Melihat sambungan jaringan di Migration Hub.

Menggunakan peran terkait layanan untuk Application Discovery Service

AWS Application Discovery Service menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis IAM role unik yang terhubung langsung ke Application Discovery Service. Peran terkait layanan telah ditentukan sebelumnya oleh Application Discovery Service dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan mempermudah persiapan Application Discovery Service karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Application Discovery Service menetapkan izin peran terkait layanan, dan kecuali jika ditentukan lain, hanya Application Discovery Service yang dapat menjalankan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Langkah ini melindungi sumber daya Application Discovery Service karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Topik

- Izin peran terkait layanan untuk Application Discovery Service
- Membuat peran terkait layanan untuk Application Discovery Service
- Menghapus peran terkait layanan untuk Application Discovery Service

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Application Discovery Service

Application Discovery Service menggunakan peran terkait layanan bernama AWSServiceRoleForApplicationDiscoveryServiceContinuousExport— Memungkinkan akses ke AWS Layanan dan Sumber Daya yang digunakan atau dikelola oleh. AWS Application Discovery Service

Peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `continuousexport.discovery.amazonaws.com`

Kebijakan izin peran tersebut mengizinkan Application Discovery Service untuk menyelesaikan tindakan berikut:

glue

- `CreateDatabase`
- `UpdateDatabase`
- `CreateTable`
- `UpdateTable`

firehose

- `CreateDeliveryStream`
- `DeleteDeliveryStream`
- `DescribeDeliveryStream`
- `PutRecord`
- `PutRecordBatch`
- `UpdateDestination`

s3

- `CreateBucket`
- `ListBucket`
- `GetObject`

log

- `CreateLogGroup`
- `CreateLogStream`
- `PutRetentionPolicy`

iam

- `PassRole`

Ini adalah kebijakan lengkap yang menunjukkan sumber daya mana yang dikenai tindakan di atas:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-
discovery-service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
```

```
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-
service/firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

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

Membuat peran terkait layanan untuk Application Discovery Service

Anda tidak perlu membuat peran terkait layanan secara manual. Peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan dibuat secara otomatis saat Ekspor Berkelanjutan diaktifkan secara implisit oleh a) opsi konfirmasi di kotak dialog yang disajikan dari halaman Pengumpul Data setelah Anda memilih “Mulai pengumpulan data”, atau klik slider berlabel, “Eksplorasi data di Athena”, atau b) saat Anda memanggil API menggunakan CLI. StartContinuousExport AWS

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Membuat peran terkait layanan dari konsol Migration Hub

Anda dapat menggunakan konsol Hub Migrasi untuk membuat peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan.

Untuk membuat peran terkait layanan (konsol)

1. Di panel navigasi, pilih Pengumpul Data.
2. Pilih tab Agen.
3. Alihkan slider Eksplorasi data di Athena ke posisi Aktif.
4. Pada kotak dialog yang dihasilkan dari langkah sebelumnya, klik kotak centang untuk menyetujui biaya terkait dan pilih Lanjutkan atau Aktifkan.

Membuat peran terkait layanan dari AWS CLI

Anda dapat menggunakan perintah Application Discovery Service dari AWS Command Line Interface untuk membuat peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan.

Peran terkait layanan ini dibuat secara otomatis saat Anda memulai Ekspor Berkelanjutan dari AWS CLI (AWS CLI harus diinstal terlebih dahulu di lingkungan Anda).

Untuk membuat peran terkait layanan (CLI) dengan memulai Ekspor Berkelanjutan dari AWS CLI

1. Instal AWS CLI untuk sistem operasi Anda (Linux, macOS, atau Windows). Lihat Panduan Pengguna AWS Command Line Interface untuk instruksi.
2. Buka Prompt perintah (Windows) atau Terminal (Linux atau macOS).
   a. Ketik `aws configure` dan tekan Enter.
   b. Masukkan ID Kunci AWS Akses dan Kunci Akses AWS Rahasia Anda.
   c. Masukkan `us-west-2` untuk Nama Wilayah Default.
   d. Masukkan `text` untuk Format Output Default.
3. Ketik perintah berikut ini:

```
aws discovery start-continuous-export
```

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan menggunakan kasus penggunaan Layanan Penemuan - Ekspor Berkelanjutan. Di IAM CLI atau IAM API, buat peran tertaut layanan dengan nama layanan `continuousexport.discovery.amazonaws.com`. Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Menghapus peran terkait layanan untuk Application Discovery Service

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan dan tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran tertaut layanan terlebih dahulu sebelum dapat menghapusnya secara manual.

Membersihkan peran terkait layanan

Sebelum dapat menggunakan IAM untuk menghapus peran tertaut-layanan, Anda harus terlebih dahulu menghapus semua sumber daya yang digunakan oleh peran tersebut.

> **Note**
>
> Jika Application Discovery Service menggunakan peran tersebut ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Application Discovery Service yang digunakan oleh peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan dari Konsol Migrasi Hub

1. Di panel navigasi, pilih Pengumpul Data.
2. Pilih tab Agen.
3. Alihkan slider Eksplorasi data di Athena ke posisi Nonaktif.

Untuk menghapus sumber daya Application Discovery Service yang digunakan oleh peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan dari AWS CLI

1. Instal AWS CLI untuk sistem operasi Anda (Linux, macOS, atau Windows). Lihat Panduan Pengguna AWS Command Line Interface untuk instruksi.
2. Buka Prompt perintah (Windows) atau Terminal (Linux atau macOS).
   a. Ketik `aws configure` dan tekan Enter.
   b. Masukkan ID Kunci AWS Akses dan Kunci Akses AWS Rahasia Anda.
   c. Masukkan `us-west-2` untuk Nama Wilayah Default.
   d. Masukkan `text` untuk Format Output Default.
3. Ketik perintah berikut ini:

```
aws discovery stop-continuous-export --export-id <export ID>
```

   - Jika Anda tidak tahu ID Ekspor dari ekspor berkelanjutan yang ingin Anda hentikan, masukkan perintah berikut untuk melihat ID ekspor berkelanjutan:

```
aws discovery describe-continuous-exports
```

4. Masukkan perintah lanjutan untuk memastikan bahwa Ekspor Berkelanjutan telah berhenti dengan memverifikasi status yang ditampilkan adalah “TIDAK AKTIF”:

```
aws discovery describe-continuous-export
```

Menghapus peran tertaut layanan secara manual

Anda dapat menghapus peran AWSService RoleForApplicationDiscoveryServiceContinuousExport terkait layanan dengan menggunakan konsol IAM, IAM CLI, atau IAM API. Jika Anda tidak perlu lagi menggunakan fitur Layanan Penemuan - Ekspor Berkelanjutan yang memerlukan peran terkait layanan ini, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak perlu lagi memantau atau memelihara entitas yang tidak digunakan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

> **Note**
>
> Anda harus membersihkan peran terkait layanan sebelum dapat menghapusnya. Lihat Membersihkan peran terkait layanan.

Pemecahan Masalah AWS Application Discovery Service Identitas dan Akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan Application Discovery Service dan IAM.

Topik

- Saya Tidak Berwenang untuk Melakukan iam: PassRole

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 Application Discovery Service.

Beberapa Layanan AWS 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 saat pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di Application Discovery Service. 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.

Logging panggilan Application Discovery Service API dengan AWS CloudTrail

AWS Application Discovery Service terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan dalam Application Discovery Service. Anda dapat menggunakan CloudTrail log, terus memantau, dan mempertahankan aktivitas akun untuk tujuan pemecahan masalah dan audit. CloudTrail menyediakan riwayat peristiwa aktivitas AWS akun Anda, termasuk tindakan yang dilakukan melalui Konsol AWS Manajemen AWS SDKs, dan alat baris perintah.

CloudTrail menangkap semua panggilan API untuk Application Discovery Service sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsol Application Discovery Service dan panggilan kode ke operasi API Application Discovery Service.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Application Discovery Service. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Application Discovery Service, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Application Discovery Service di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Application Discovery Service, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Application Discovery Service, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran Umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua tindakan Application Discovery Service dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Application Discovery Service. Misalnya, panggilan ke`CreateTags`,`DescribeTags`, dan `GetDiscoverySummary` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami entri berkas log Application Discovery Service

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `DescribeTags` tindakan.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
        "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAJQABLZS4A3QDU576Q",
                "arn": "arn:aws:iam::444455556666:role/ReadOnly",
                "accountId": "444455556666",
                "userName": "sampleAdmin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-05-05T15:19:03Z"
            }
        }
    },
    "eventTime": "2020-05-05T17:02:40Z",
    "eventSource": "discovery.amazonaws.com",
    "eventName": "DescribeTags",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "20.22.33.44",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
```

```
        "maxResults": 0,
        "filters": [
            {
                "values": [
                    "d-server-0315rfdjreyqsq"
                ],
                "name": "configurationId"
            }
        ]
    },
    "responseElements": null,
    "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
    "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

AWS Application Discovery Service Format ARN

Amazon Resource Name (ARN) adalah string yang secara unik mengidentifikasi sumber daya. AWS AWS memerlukan ARN saat Anda ingin menentukan sumber daya secara jelas di semua. AWS AWS Application Discovery Service mendefinisikan yang berikut ARNs ini.

- Agen Penemuan: `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- Kolektor Tanpa Agen: `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- Kolektor Evaluator Migrasi: `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Konektor Penemuan: `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service Kuota

Konsol Service Quotas memberikan informasi tentang AWS Application Discovery Service kuota. Anda dapat menggunakan konsol Service Quotas untuk melihat kuota layanan default atau mengajukan penambahan kuota untuk kuota yang dapat disesuaikan.

Saat ini, satu-satunya kuota yang dapat ditambah adalah server yang diimpor per akun.

Application Discovery Service memiliki kuota default berikut:

- 1.000 aplikasi per akun.

  Jika Anda mencapai kuota ini, dan ingin mengimpor aplikasi baru, Anda dapat menghapus aplikasi yang sudah ada dengan tindakan API `DeleteApplications`. Untuk informasi selengkapnya, lihat DeleteApplicationsdi Referensi API Application Discovery Service.
- Setiap file impor dapat memiliki ukuran file maksimum 10 MB.
- 25.000 catatan server yang diimpor per akun.
- 25.000 penghapusan catatan impor per hari.
- 10.000 server yang diimpor per akun (Anda dapat meminta untuk menambah kuota ini).
- 1.000 agen aktif, yang mengumpulkan dan mengirim data ke Application Discovery Service.
- 10.000 agen tidak aktif, yang responsif tetapi tidak mengumpulkan data.
- 400 server per aplikasi.
- 30 tag per server.

Pemecahan masalah AWS Application Discovery Service

Di bagian ini, Anda dapat menemukan informasi tentang cara memperbaiki masalah umum dengan AWS Application Discovery Service.

Topik

- Hentikan pengumpulan data dengan eksplorasi data
- Hapus data yang dikumpulkan oleh eksplorasi data
- Perbaiki masalah umum dengan eksplorasi data di Amazon Athena
- Memecahkan masalah catatan impor yang gagal

Hentikan pengumpulan data dengan eksplorasi data

Untuk menghentikan eksplorasi data, Anda dapat mematikan sakelar sakelar di konsol Migration Hub di bawah tab Discover > Data Collectors > Agents, atau menjalankan API. `StopContinuousExport` Diperlukan waktu hingga 30 menit untuk menghentikan pengumpulan data, dan selama tahap ini, sakelar sakelar di konsol dan pemanggilan `DescribeContinuousExport` API akan menampilkan status eksplorasi data sebagai “Stop In Progress”.

> **Note**
>
> Jika setelah menyegarkan halaman konsol, toggle tidak mati dan muncul pesan kesalahan atau API `DescribeContinuousExport` menghasilkan status “Penghentian_Gagal”, Anda dapat mencoba lagi dengan mematikan tombol toggle atau memanggil API `StopContinuousExport`. Jika “eksplorasi data” masih menunjukkan kesalahan dan gagal berhasil berhenti, hubungi AWS dukungan.

Selain itu, Anda dapat menghentikan pengumpulan data secara manual seperti yang dijelaskan dalam langkah-langkah berikut.

Opsi 1: Hentikan pengumpulan Agent Data

Jika Anda telah menyelesaikan pencarian menggunakan agen ADS dan tidak lagi ingin mengumpulkan data tambahan di repositori basis data ADS:

1. Dari konsol Migration Hub, pilih tab Temukan > Pengumpul Data > Agen.

2. Pilih semua agen yang sedang beroperasi lalu pilih Hentikan Pengumpulan Data.

   Ini akan memastikan bahwa tidak ada data baru yang dikumpulkan oleh agen di repositori data ADS dan bucket S3 Anda. Data yang ada tetap dapat diakses.

Opsi 2: Hapus Amazon Kinesis Data Streams eksplorasi data

Jika Anda ingin terus mengumpulkan data oleh agen di repositori data ADS, tetapi tidak ingin mengumpulkan data di bucket Amazon S3 menggunakan eksplorasi data, Anda dapat secara manual menghapus aliran Amazon Data Firehose yang dibuat oleh eksplorasi data:

1. Masuk ke Amazon Kinesis dari AWS konsol dan pilih Data Firehose dari panel navigasi.
2. Hapus aliran berikut yang dibuat oleh fitur eksplorasi data:

   - `aws-application-discovery-service-id_mapping_agent`
   - `aws-application-discovery-service-inbound_connection_agent`
   - `aws-application-discovery-service-network_interface_agent`
   - `aws-application-discovery-service-os_info_agent`
   - `aws-application-discovery-service-outbound_connection_agent`
   - `aws-application-discovery-service-processes_agent`
   - `aws-application-discovery-service-sys_performance_agent`

Hapus data yang dikumpulkan oleh eksplorasi data

Untuk menghapus data yang dikumpulkan oleh eksplorasi data

1. Hapus data agen penemuan yang disimpan di Amazon S3.

   Data yang dikumpulkan oleh AWS Application Discovery Service (ADS) disimpan dalam bucket S3 bernama`aws-application-discover-discovery-service-`*`uniqueid`*.

   > **Note**
   >
   > Menghapus bucket Amazon S3 atau objek apa pun di dalamnya saat eksplorasi data di Amazon Athena diaktifkan menyebabkan kesalahan. Ini terus mengirim data agen penemuan baru ke S3. Data yang dihapus tidak lagi dapat diakses di Athena.

2. Hapus AWS Glue Data Catalog.

   Saat eksplorasi data di Amazon Athena diaktifkan, ia akan membuat bucket Amazon S3 di akun Anda untuk menyimpan data yang dikumpulkan oleh agen ADS secara berkala. Selain itu, ini juga membuat AWS Glue Data Catalog untuk memungkinkan Anda menanyakan data yang disimpan dalam ember Amazon S3 dari Amazon Athena. Saat Anda mematikan eksplorasi data di Amazon Athena, tidak ada data baru yang disimpan di bucket Amazon S3 Anda, tetapi data yang dikumpulkan sebelumnya akan tetap ada. Jika Anda tidak lagi memerlukan data ini dan ingin mengembalikan akun Anda ke negara bagian sebelum eksplorasi data di Amazon Athena diaktifkan.

   a. Kunjungi Amazon S3 dari AWS konsol dan hapus bucket secara manual dengan nama "aws-application-discover-discovery-service-uniqueid”

   b. Anda dapat secara manual menghapus eksplorasi data AWS Glue Data Catalog dengan menghapus application-discovery-service-databasedatabase dan semua tabel ini:

      - `os_info_agent`
      - `network_interface_agent`
      - `sys_performance_agent`
      - `processes_agent`
      - `inbound_connection_agent`
      - `outbound_connection_agent`
      - `id_mapping_agent`

Menghapus data Anda dari AWS Application Discovery Service

Agar semua data Anda dihapus dari Application Discovery Service, hubungi AWS Support dan minta penghapusan data lengkap.

Perbaiki masalah umum dengan eksplorasi data di Amazon Athena

Di bagian ini, Anda dapat menemukan informasi tentang cara memperbaiki masalah umum dengan eksplorasi data di Amazon Athena.

Topik

- Eksplorasi data di Amazon Athena gagal dimulai karena peran terkait layanan dan AWS sumber daya yang diperlukan tidak dapat dibuat
- Data Agen Baru tidak muncul di Amazon Athena
- Anda tidak memiliki izin yang cukup untuk mengakses Amazon S3, Amazon Data Firehose, atau AWS Glue

Eksplorasi data di Amazon Athena gagal dimulai karena peran terkait layanan dan AWS sumber daya yang diperlukan tidak dapat dibuat

Saat Anda mengaktifkan eksplorasi data di Amazon Athena, itu akan menciptakan peran terkait layanan`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`, di akun Anda yang memungkinkannya membuat sumber daya yang AWS diperlukan untuk membuat data yang dikumpulkan agen dapat diakses di Amazon Athena termasuk bucket Amazon S3, aliran Amazon Kinesis, dan. AWS Glue Data Catalog Jika akun Anda tidak memiliki izin yang tepat untuk eksplorasi data di Amazon Athena untuk membuat peran ini, itu akan gagal untuk diinisialisasi. Lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.

Data Agen Baru tidak muncul di Amazon Athena

Jika data baru tidak mengalir ke Athena, sudah lebih dari 30 menit sejak agen memulai, dan status eksplorasi data Aktif, periksa solusi yang tercantum di bawah ini:

- AWS Agen Penemuan

  Pastikan bahwa status Pengumpulan pada agen Anda Dimulai dan status Kondisi ditandai sebagai Berjalan.

- Peran Kinesis

  Pastikan Anda memiliki peran `AWSApplicationDiscoveryServiceFirehose` di akun Anda.

- Status Firehose

  Pastikan aliran pengiriman Firehose berikut berfungsi dengan benar:

  - `aws-application-discovery-service/os_info_agent`
  - `aws-application-discovery-service-network_interface_agent`

  - `aws-application-discovery-service-sys_performance_agent`
  - `aws-application-discovery-service-processes_agent`
  - `aws-application-discovery-service-inbound_connection_agent`
  - `aws-application-discovery-service-outbound_connection_agent`
  - `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

  Pastikan `application-discovery-service-database` database ada di dalamnya AWS Glue. Pastikan bahwa tabel berikut ini ada di AWS Glue:

  - `os_info_agent`
  - `network_interface_agent`
  - `sys_performance_agent`
  - `processes_agent`
  - `inbound_connection_agent`
  - `outbound_connection_agent`
  - `id_mapping_agent`

- Bucket Amazon S3

  Pastikan Anda memiliki bucket Amazon S3 bernama `aws-application-discovery-service-`*`uniqueid`* di akun Anda. Jika objek dalam bucket telah dipindahkan atau dihapus, objek tidak akan muncul dengan benar di Athena.

- Server on-premise Anda

  Pastikan server Anda berjalan sehingga agen Anda dapat mengumpulkan dan mengirim data ke AWS Application Discovery Service.

Anda tidak memiliki izin yang cukup untuk mengakses Amazon S3, Amazon Data Firehose, atau AWS Glue

Jika Anda menggunakan AWS Organizations, dan inisialisasi untuk eksplorasi data di Amazon Athena gagal, itu bisa karena Anda tidak memiliki izin untuk mengakses Amazon S3, Amazon Data Firehose, Athena atau. AWS Glue

Anda akan memerlukan pengguna IAM dengan izin administrator yang dapat memberi Anda akses ke layanan ini. Administrator dapat menggunakan akun mereka untuk memberikan akses ini. Lihat AWS kebijakan terkelola untuk AWS Application Discovery Service.

Untuk memastikan bahwa eksplorasi data di Amazon Athena berfungsi dengan benar, jangan mengubah atau menghapus sumber daya yang dibuat oleh eksplorasi data AWS di Amazon Athena termasuk bucket Amazon S3, Amazon Data Firehose Streams, dan. AWS Glue Data Catalog Jika Anda secara tidak sengaja menghapus atau mengubah sumber daya ini, hentikan dan mulai Eksplorasi Data. Sumber daya ini akan secara otomatis dibuat lagi. Jika Anda menghapus bucket Amazon S3 yang dibuat oleh eksplorasi data, Anda mungkin kehilangan data yang dikumpulkan di bucket.

Memecahkan masalah catatan impor yang gagal

Impor Migration Hub memungkinkan Anda mengimpor detail lingkungan on-premise secara langsung ke Migration Hub tanpa menggunakan Discovery Connector atau Discovery Agent. Anda diberi pilihan untuk melakukan penilaian dan perencanaan migrasi langsung dari data yang Anda impor. Anda juga dapat mengelompokkan perangkat sebagai aplikasi dan melacak status migrasinya.

Saat mengimpor data, mungkin terjadi beberapa kesalahan. Biasanya, kesalahan ini terjadi karena salah satu alasan berikut:

- Kuota terkait impor sudah tercapai – Ada kuota yang terkait dengan tugas impor. Jika Anda membuat permintaan tugas impor yang akan melebihi kuota, maka permintaan akan gagal dan menghasilkan kesalahan. Untuk informasi selengkapnya, lihat AWS Application Discovery Service Kuota.
- Koma tambahan (,) masuk ke file impor – Koma dalam file .CSV digunakan untuk membedakan satu bidang dari bidang berikutnya. Koma yang muncul dalam bidang tidak didukung karena tanda ini akan selalu membagi bidang. Hal ini dapat menyebabkan serangkaian kesalahan format. Pastikan koma hanya digunakan di antara bidang, dan tidak digunakan dalam file impor Anda.

- Sebuah bidang memiliki nilai di luar rentang yang didukung – Beberapa bidang, seperti `CPU.NumberOfCores` harus memiliki rentang nilai yang didukung. Jika Anda memiliki nilai yang lebih atau kurang dari rentang yang didukung ini, maka catatan akan gagal diimpor.

Jika terjadi kesalahan pada permintaan impor, Anda dapat mengatasinya dengan mengunduh catatan kegagalan tugas impor, dan memperbaiki kesalahan tersebut dalam file CSV entri yang gagal, dan melakukan impor lagi.

Console

Untuk mengunduh arsip catatan kegagalan

1. Masuk ke Konsol Manajemen AWS, dan buka konsol Migration Hub dihttps://console.aws.amazon.com/migrationhub.
2. Dari navigasi sisi kiri, di bawah Temukan, pilih Alat.
3. Dari Alat Penemuan, pilih lihat impor.
4. Dari dasbor Impor, pilih tombol radio terkait permintaan impor dengan sejumlah Catatan kegagalan.
5. Pilih Unduh catatan kegagalan dari atas tabel di dasbor. Tindakan ini akan membuka kotak dialog unduhan pada peramban Anda untuk mengunduh file arsip.

AWS CLI

Untuk mengunduh arsip catatan kegagalan

1. Buka jendela terminal, dan ketik perintah berikut, di mana *`ImportName`* `is the name of the import task with the failed entries that you want to correct.`:

   ```
   aws discovery describe-import-tasks - -name ImportName
   ```

2. Dari output tersebut, salin seluruh isi nilai yang dihasilkan untuk `errorsAndFailedEntriesZip`, tanpa tanda kutip yang mengapitnya.
3. Buka peramban web, lalu tempel isi ke kotak teks URL dan tekan `ENTER`. Tindakan ini akan mengunduh arsip catatan kegagalan, yang dikompresi dalam format .zip.

Setelah mengunduh arsip catatan kegagalan, Anda dapat mengekstraksi kedua file di dalamnya dan memperbaiki kesalahannya. Perhatikan bahwa jika kesalahan terkait dengan batas berbasis layanan,

Anda harus meminta peningkatan batas, atau menghapus beberapa sumber daya terkait supaya akun Anda tidak melebihi batas. Arsip tersebut memiliki file-file berikut:

- errors-file.csv – File ini adalah log kesalahan yang melacak baris, nama kolom, `ExternalId`, dan pesan kesalahan deskriptif untuk setiap catatan kegagalan dari setiap entri yang gagal.
- failed-entries-file.csv - File ini hanya berisi entri gagal dari file impor asli Anda.

Untuk memperbaiki non-limit-based kesalahan yang Anda temui, gunakan `errors-file.csv` untuk memperbaiki masalah dalam `failed-entries-file.csv` file, lalu impor file itu. Untuk petunjuk tentang mengimpor file, lihat Mengimpor data.

Riwayat Dokumen untuk AWS Application Discovery Service

Pembaruan dokumentasi Panduan Pengguna terbaru: 16 Mei 2023

Tabel berikut menjelaskan perubahan penting pada Panduan Pengguna Application Discovery Service setelah 18 Januari 2019. Untuk notifikasi tentang pembaruan dokumentasi, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Mode pemeliharaan	AWS Application Discovery Service tidak lagi terbuka untuk pelanggan baru. Atau, gunakan AWS Transform yang menyediakan kemampuan serupa. Untuk informasi selengkapnya, lihat perubahan ketersediaan AWS Application Discovery Service.	November 7, 2025
Transisi dari Discovery Connector ke Agentless Collector	Kami menyarankan agar pelanggan yang saat ini menggunakan Discovery Connector beralih ke Agentless Collector baru. Mulai 17 November 2025, AWS Application Discovery Service akan berhenti menerima data baru dari Discovery Connectors. Untuk informasi selengkapnya, lihat Discovery Connector.	November 12, 2024
Merilis modul Pengumpulan Data Jaringan Kolektor Tanpa Agen	Modul Pengumpulan Data Jaringan memungkinkan Anda menemukan dependens i di antara server di pusat	November 8, 2024

	data lokal Anda. Untuk informasi selengkapnya, lihat Menggunakan modul Pengumpulan Data Jaringan Kolektor Tanpa Agen.	
Support untuk pengumpulan tanpa agen untuk pemetaan ketergantungan	Untuk informasi selengkapnya, lihat Menggunakan modul pengumpulan data VMware vCenter Agentless Collector.	Oktober 24, 2024
Dirilis Agentless Collector versi 2 berdasarkan Amazon Linux 2023	Untuk informasi lebih lanjut, lihat Prasyarat untuk Kolektor Tanpa Agen.	September 26, 2024
Prasyarat Kolektor Tanpa Agen yang Diperbarui	Untuk informasi lebih lanjut, lihat Prasyarat untuk Kolektor Tanpa Agen.	September 9, 2024
Konsistensi akhirnya di API	Untuk informasi selengkapnya, lihat Konsistensi akhir di AWS Application Discovery Service API.	Juni 20, 2024
Pembaruan Kolektor Tanpa Agen	Kami menambahkan `sts.amazonaws.com` ke daftar domain yang memerlukan akses keluar. Untuk informasi selengkapnya, lihat Mengonfigurasi firewall untuk akses keluar ke domain AWS.	Juni 20, 2024
Untuk memisahkan akses, buat dan gunakan akun AWS terpisah.	Untuk informasi selengkapnya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS Application Discovery Service.	April 5, 2024

Memperkenalkan database Agentless Collector dan modul pengumpulan data analitik	Modul pengumpulan data database dan analitik adalah modul baru dari Application Discovery Service Agentless Collector (Agentless Collector). Anda dapat menggunakan modul pengumpulan data ini untuk terhubung ke lingkunga n Anda dan mengumpulkan metadata dan metrik kinerja dari database lokal dan server analitik. Untuk informasi selengkapnya, lihat Modul pengumpulan data database dan analitik.	16 Mei 2023
Memperkenalkan Application Discovery Service Agentless Collector	Application Discovery Service Agentless Collector (Agentless Collector) adalah aplikasi AWS Application Discovery Service lokal baru yang mengumpul kan informasi melalui metode tanpa agen tentang lingkunga n lokal Anda untuk membantu Anda merencanakan migrasi ke lokasi secara efektif. AWS Cloud Untuk informasi lebih lanjut, lihat Agentless Collector .	Agustus 16, 2022

Pembaruan IAM	`discovery:GetNetworkConnectionGraph` Tindakan AWS Identity and Access Management (IAM) sekarang tersedia untuk memberikan akses ke diagram jaringan AWS Migration Hub konsol saat membuat kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat Memberikan izin untuk menggunakan diagram jaringan.	24 Mei 2022
Memperkenalkan Wilayah asal	Wilayah beranda Hub Migrasi menyediakan satu repositori informasi penemuan dan perencanaan migrasi untuk seluruh portofolio Anda, dan satu tampilan migrasi ke beberapa Wilayah. AWS	20 November 2019
Memperkenalkan fitur impor Migration Hub	Impor Migration Hub mengizinkan Anda mengimpor informasi tentang server dan aplikasi on-premise ke Migration Hub, termasuk spesifikasi server dan pemanfaatan data. Anda juga dapat menggunakan data ini untuk melacak status migrasi aplikasi. Untuk informasi selengkapnya, lihat Impor Migration Hub.	18 Januari 2019

Tabel berikut menjelaskan rilis dokumentasi untuk Panduan Pengguna Application Discovery Service sebelum 18 Januari 2019:

Ubah	Deskripsi	Date
Fitur Baru	Dokumen yang diperbarui untuk mendukung eksploras i data di Amazon Athena dan menambahkan chapter Pemecahan Masalah.	9 Agustus 2018
Revisi besar	Penulisan ulang detail penggunaan & output; seluruh dokumen direstrukturisasi.	25 Mei 2018
Discovery Agent 2.0	Aplikasi Discovery Agent baru dan ditingkatkan telah dirilis.	19 Oktober 2017
Konsol	Konsol Manajemen AWS Itu ditambahkan.	19 Desember 2016
Penemuan tanpa agen	Rilis ini menjelaskan cara menyiapkan dan mengonfig urasi penemuan tanpa agen.	28 Juli 2016
Detail baru untuk Microsoft Windows Server dan perbaikan masalah perintah	Pembaruan ini menambahk an detail tentang Microsoft Windows Server. Pembaruan ini juga mendokumentasikan perbaikan untuk berbagai masalah perintah.	20 Mei 2016
Publikasi awal	Ini adalah rilis pertama Panduan pengguna Applicati on Discovery Service.	12 Mei 2016

AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS

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