Panduan Administrasi

AWS Directory Service

Versi 1.0

AWS Directory Service: Panduan Administrasi

Table of Contents

Apa itu AWS Directory Service?

AWS Directory Service menyediakan beberapa cara untuk menggunakan Microsoft Active Directory (AD) dengan AWS layanan lain. Direktori menyimpan informasi tentang pengguna, grup, dan perangkat, dan administrator menggunakannya untuk mengelola akses ke informasi dan sumber daya. AWS Directory Service menyediakan beberapa pilihan direktori untuk pelanggan yang ingin menggunakan aplikasi sadar Microsoft AD atau Lightweight Directory Access Protocol (LDAP) yang ada di cloud. Ini juga menawarkan pilihan yang sama untuk developer yang membutuhkan direktori untuk mengelola pengguna, grup, perangkat, dan akses.

Mana yang harus dipilih

Anda dapat memilih layanan direktori dengan fitur dan skalabilitas yang paling sesuai dengan kebutuhan Anda. Gunakan tabel berikut untuk membantu Anda menentukan opsi AWS Directory Service direktori mana yang paling cocok untuk organisasi Anda.

Apa yang perlu Anda lakukan?	AWS Directory Service Opsi yang disarankan
Saya memerlukan Direktori Aktif atau LDAP untuk aplikasi saya di cloud	Gunakan AWS Directory Service untuk Microsoft Active Directory (Edisi Standar atau Edisi Perusahaan) jika Anda memerlukan aktual Microsoft Active Directory di AWS Cloud yang mendukung Active Directory beban kerja yang sadar, atau AWS aplikasi dan layanan seperti Amazon dan WorkSpaces Amazon QuickSight, atau Anda memerlukan dukungan LDAP untuk aplikasi Linux. Gunakan AD Connector jika Anda hanya perlu mengizink an pengguna lokal untuk masuk ke AWS aplikasi dan layanan dengan Active Directory kredensialnya. Anda juga dapat menggunakan AD Connector untuk menggabungkan instans Amazon EC2 ke domain yang sudah ada. Active Directory Gunakan Simple AD jika Anda memerlukan direktori berskala rendah dan berbiaya rendah dengan Active Directory kompatibilitas dasar yang mendukung aplikasi

Apa yang perlu Anda lakukan?	AWS Directory Service Opsi yang disarankan
	yang kompatibel dengan Samba 4, atau Anda memerlukan kompatibilitas LDAP untuk aplikasi yang sadar LDAP.
Saya mengembangkan aplikasi SaaS	Gunakan Amazon Cognito jika Anda mengembangkan aplikasi SaaS skala tinggi dan memerlukan direktori yang dapat diskalakan untuk mengelola dan mengautentikasi pelanggan Anda dan yang berfungsi dengan identitas media sosial.

Untuk informasi selengkapnya tentang opsi AWS Directory Service direktori, lihat Cara memilih Active Directory solusi AWS.

AWS Directory Service pilihan

AWS Directory Service mencakup beberapa jenis direktori untuk dipilih. Untuk informasi selengkapnya, pilih salah satu dari tab berikut:

AWS Directory Service for Microsoft Active Directory

Juga dikenal sebagai AWS Managed Microsoft AD, AWS Directory Service untuk Microsoft Active Directory didukung oleh aktual Microsoft Windows Server Active Directory (AD), dikelola oleh AWS di AWS Cloud. Ini memungkinkan Anda untuk memigrasikan berbagai aplikasi Active Directory—aware ke Cloud. AWS AWS Microsoft AD yang dikelola bekerja denganMicrosoft SharePoint, Microsoft SQL Server Always On Availability Groups, dan banyak aplikasi.NET. Ini juga mendukung aplikasi dan layanan AWS terkelola termasuk Amazon WorkSpaces, Amazon, Amazon WorkDocs, Amazon Chime QuickSight, Amazon Connect, dan Amazon Relational Database Service untuk (Amazon RDS for, Microsoft SQL Server Amazon RDS forSQL Server, dan Amazon RDS Oracle for PostgreSQL).

AWS Microsoft AD yang dikelola disetujui untuk aplikasi di AWS Cloud yang tunduk pada kepatuhan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS (HIPAA) atau Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) saat Anda mengaktifkan kepatuhan untuk direktori Anda.

Semua aplikasi yang kompatibel bekerja dengan kredensyal pengguna yang Anda simpan di AWS Microsoft AD Terkelola, atau Anda dapat terhubung ke infrastruktur AD yang ada dengan kepercayaan dan menggunakan kredensyal dari Windows yang Active Directory berjalan di tempat atau di EC2 Windows. Jika Anda menggabungkan instans EC2 ke AWS Microsoft AD Terkelola, pengguna dapat mengakses beban kerja Windows di AWS Cloud dengan pengalaman masuk tunggal (SSO) Windows yang sama seperti saat mereka mengakses beban kerja di jaringan lokal Anda.

AWS Microsoft AD yang dikelola juga mendukung kasus penggunaan federasi menggunakan Active Directory kredensyal. Sendiri, Microsoft AD yang AWS Dikelola memungkinkan Anda masuk ke file AWS Management Console. Dengan AWS IAM Identity Center, Anda juga dapat memperoleh kredensyal jangka pendek untuk digunakan dengan AWS SDK dan CLI, dan menggunakan integrasi SAMP yang telah dikonfigurasi sebelumnya untuk masuk ke banyak aplikasi cloud. Dengan menambahkan Microsoft Entra Connect (sebelumnya dikenal sebagaiAzure Active Directory Connect), dan secara opsional Active Directory Federation Service (AD FS), Anda dapat masuk ke Microsoft Office 365 dan aplikasi cloud lainnya dengan kredensyal yang disimpan di Microsoft AD yang Dikelola. AWS

Layanan ini mencakup fitur-fitur utama yang memungkinkan Anda untuk Memperpanjang skema Anda, Mengelola kebijakan kata sandi, dan mengaktifkan komunikasi LDAP yang aman melalui Lapisan Soket Aman (SSL)/Keamanan Lapisan Pengangkutan (TLS). Anda juga dapat mengaktifkan otentikasi multi-faktor (MFA) untuk AWS Microsoft AD yang Dikelola untuk memberikan lapisan keamanan tambahan saat pengguna mengakses AWS aplikasi dari Internet. Karena Active Directory merupakan direktori LDAP, Anda juga dapat menggunakan otentikasi AWS Managed Microsoft AD for Linux Secure Shell (SSH) dan untuk aplikasi lain yang mendukung LDAP.

AWS menyediakan pemantauan, snapshot harian, dan pemulihan sebagai bagian dari layanan —Anda menambahkan pengguna dan grup ke AWS Microsoft AD yang Dikelola, dan mengelola Kebijakan Grup menggunakan Active Directory alat familiar yang berjalan di Windows komputer yang bergabung dengan domain Microsoft AD Terkelola AWS . Anda juga dapat menskalakan direktori dengan men-deploy pengendali domain tambahan dan membantu meningkatkan performa aplikasi dengan mendistribusikan permintaan di sejumlah besar pengendali domain.

AWS Microsoft AD yang dikelola tersedia dalam dua edisi: Standar dan Perusahaan.

- Edisi Standar: Microsoft AD yang Dikelola AWS (Edisi Standar) dioptimalkan untuk menjadi direktori primer untuk bisnis kecil dan menengah sampai dengan 5.000 karyawan. Ini

menyediakan kapasitas penyimpanan yang cukup untuk mendukung hingga 30.000* objek direktori, seperti pengguna, grup, dan komputer.

- Edisi Enterprise: Microsoft AD yang Dikelola AWS (Edisi Enterprise) dirancang untuk mendukung organisasi korporasi dengan hingga 500.000* direktori objek.

* batas atas adalah perkiraan. Direktori Anda mungkin mendukung lebih atau kurang objek direktori tergantung pada ukuran objek Anda dan perilaku dan kebutuhan performa aplikasi Anda.

Kapan harus digunakan

AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memerlukan Active Directory fitur aktual untuk mendukung AWS aplikasi atau Windows beban kerja, termasuk Amazon Relational Database Service untuk. Microsoft SQL Server Ini juga terbaik jika Anda ingin mandiri Active Directory di AWS Cloud yang mendukung Office 365 atau Anda memerlukan direktori LDAP untuk mendukung aplikasi Linux Anda. Untuk informasi selengkapnya, lihat AWS Microsoft AD yang dikelola.

AD Connector

AD Connector adalah layanan proxy yang menyediakan cara mudah untuk menghubungkan AWS aplikasi yang kompatibel, seperti Amazon WorkSpaces, Amazon QuickSight, dan Amazon EC2 untuk Windows Server instans, ke lokal yang ada. Microsoft Active Directory Dengan AD Connector, Anda cukup menambahkan satu akun layanan ke akun AndaActive Directory. AD Connector juga menghilangkan kebutuhan sinkronisasi direktori atau biaya dan kompleksitas hosting infrastruktur federasi.

Saat Anda menambahkan pengguna ke AWS aplikasi seperti Amazon QuickSight, AD Connector akan membaca yang ada Active Directory untuk membuat daftar pengguna dan grup yang dapat dipilih. Saat pengguna masuk ke AWS aplikasi, AD Connector meneruskan permintaan masuk ke pengontrol Active Directory domain lokal untuk autentikasi. AD Connector bekerja dengan banyak AWS aplikasi dan layanan termasuk Amazon WorkSpaces, Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect, dan Amazon. WorkMail Anda juga dapat menggabungkan Windows instans EC2 ke domain lokal melalui AD Connector menggunakan gabungan Active Directory domain tanpa batas. AD Connector juga memungkinkan pengguna Anda mengakses AWS Management Console dan mengelola AWS sumber daya dengan masuk dengan Active Directory kredensialnya yang ada. AD Connector tidak kompatibel dengan RDS SQL Server.

Anda juga dapat menggunakan AD Connector untuk mengaktifkan otentikasi multi-faktor (MFA) bagi pengguna AWS aplikasi Anda dengan menghubungkannya ke infrastruktur MFA berbasis Radius yang ada. Ini memberikan lapisan keamanan tambahan saat pengguna mengakses aplikasi AWS .

Dengan AD Connector, Anda terus mengelola Active Directory seperti yang Anda lakukan sekarang. Misalnya, Anda menambahkan pengguna dan grup baru dan memperbarui kata sandi menggunakan alat Active Directory administrasi standar di lokasi AndaActive Directory. Ini membantu Anda menerapkan kebijakan keamanan secara konsisten, seperti kedaluwarsa kata sandi, riwayat kata sandi, dan penguncian akun, baik pengguna mengakses sumber daya di tempat maupun di Cloud. AWS

Kapan harus digunakan

AD Connector adalah pilihan terbaik Anda saat ingin menggunakan direktori lokal yang ada dengan AWS layanan yang kompatibel. Untuk informasi selengkapnya, lihat AD Connector.

Simple AD

Simple AD adalah Microsoft Active Directory direktori yang kompatibel dari AWS Directory Service yang didukung oleh Samba 4. Simple AD mendukung Active Directory fitur dasar seperti akun pengguna, keanggotaan grup, bergabung dengan domain Linux atau instans EC2 Windows berbasis, SSO berbasis Kerberos, dan kebijakan grup. AWS menyediakan pemantauan, snap-shot harian, dan pemulihan sebagai bagian dari layanan.

Simple AD adalah direktori mandiri di cloud, di mana Anda membuat dan mengelola identitas pengguna dan mengelola akses ke aplikasi. Anda dapat menggunakan banyak aplikasi dan alat yang sudah dikenal Active Directory yang membutuhkan Active Directory fitur dasar. Simple AD kompatibel dengan AWS aplikasi berikut: Amazon WorkSpaces, Amazon WorkDocs, Amazon QuickSight, dan Amazon WorkMail. Anda juga dapat masuk ke akun pengguna Simple AD AWS Management Console dengan Simple AD dan mengelola AWS sumber daya.

Simple AD tidak mendukung otentikasi multi-faktor (MFA), hubungan kepercayaan, pembaruan dinamis DNS, ekstensi skema, komunikasi melalui LDAPS, cmdlet AD, atau transfer peran FSMO. PowerShell Simple AD tidak kompatibel dengan RDS SQL Server. Pelanggan yang memerlukan fitur aktual MicrosoftActive Directory, atau yang membayangkan menggunakan direktori mereka dengan RDS SQL Server harus menggunakan Managed AWS Microsoft AD sebagai gantinya. Pastikan aplikasi yang Anda butuhkan kompatibel sepenuhnya dengan Samba 4 sebelum menggunakan Simple AD. Untuk informasi selengkapnya, lihat https://www.samba.org.

Kapan harus digunakan

Anda dapat menggunakan Simple AD sebagai direktori mandiri di cloud untuk mendukung Windows beban kerja yang memerlukan Active Directory fitur dasar, AWS aplikasi yang kompatibel, atau untuk mendukung beban kerja Linux yang memerlukan layanan LDAP. Untuk informasi selengkapnya, lihat Simple AD.

Amazon Cognito

Amazon Cognito adalah direktori pengguna yang menambahkan pendaftaran dan masuk ke aplikasi seluler atau aplikasi web Anda menggunakan Kumpulan Pengguna Amazon Cognito.

Kapan harus digunakan

Anda juga dapat menggunakan Amazon Cognito ketika Anda perlu membuat bidang pendaftaran kustom dan menyimpan metadata dalam direktori pengguna Anda. Layanan terkelola penuh ini menskalakan untuk mendukung ratusan juta pengguna. Untuk informasi lebih lanjut, lihat Kolam pengguna Amazon Cognito di Panduan Developer Amazon Cognito.

Lihat Ketersediaan wilayah untuk AWS Directory Service untuk daftar jenis direktori yang didukung per Region.

Bekerja dengan Amazon EC2

Sebuah pemahaman dasar Amazon EC2 sangat penting untuk menggunakan AWS Directory Service. Kami menyarankan Anda untuk memulai dengan membaca topik berikut:

- Apa itu Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
- Meluncurkan instans EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
- Grup Keamanan di Panduan Pengguna Amazon EC2 untuk Instans Windows.
- Apa itu Amazon VPC? di Panduan Pengguna Amazon VPC.
- Menambahkan Hardware Gateway Privat Virtual ke VPC Anda di Panduan Pengguna Amazon VPC.

Memulai dengan AWS Directory Service

Jika Anda belum melakukannya, Anda juga harus membuat AWS akun dan menggunakan AWS Identity and Access Management layanan untuk mengontrol akses.

Untuk bekerja dengan AWS Directory Service, Anda harus memenuhi prasyarat untuk Directory AWS Service untuk Microsoft Active Directory, AD Connector, atau Simple AD. Untuk informasi selengkapnya, lihat AWS Prasyarat Microsoft AD yang dikelola, Prasyarat AD Connector, atau Prasyarat Simple AD.

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

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

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

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

Membuat pengguna administratif

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

Amankan Pengguna root akun AWS

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

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root dalam Panduan PenggunaAWS Sign-In .
2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

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

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

Masuk sebagai pengguna administratif

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

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

Informasi Selengkapnya

- Untuk informasi selengkapnya tentang cara masuk ke AWS Management Console sebagai pengguna Pusat Identitas IAM, lihat Masuk ke portal akses Pusat Identitas IAM.

- Untuk informasi selengkapnya tentang cara masuk ke pengguna IAM AWS Management Console sebagai, lihat Masuk ke pengguna IAM AWS Management Console sebagai.
- Untuk informasi selengkapnya tentang penggunaan kebijakan IAM untuk mengontrol akses ke AWS Directory Service sumber daya Anda, lihatMenggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Directory Service.

AWS Microsoft AD yang dikelola

AWS Directory Service memungkinkan Anda menjalankan Microsoft Active Directory (AD) sebagai layanan terkelola. AWS Directory Service untuk Microsoft Active Directory, juga disebut sebagai AWS Managed Microsoft AD, didukung oleh Windows Server 2019. Ketika Anda memilih dan meluncurkan jenis direktori ini, itu dibuat sebagai sepasang pengontrol domain yang sangat tersedia yang terhubung ke cloud pribadi virtual Anda (Amazon VPC). Pengendali domain yang berjalan di Availability Zone yang berbeda di Region pilihan Anda. Host pemantauan dan pemulihan, replikasi data, snapshot, dan pembaruan perangkat lunak yang secara otomatis dikonfigurasi dan dikelola untuk Anda.

Dengan Microsoft AD yang AWS Dikelola, Anda dapat menjalankan beban kerja yang sadar direktori di AWS Cloud, termasuk aplikasi berbasis .NET Microsoft SharePoint dan SQL Server kustom. Anda juga dapat mengonfigurasi hubungan kepercayaan antara Microsoft AD yang AWS Dikelola di AWS Cloud dan lokal yang ada MicrosoftActive Directory, yang memberikan pengguna dan grup akses ke sumber daya di salah satu domain, menggunakan AWS IAM Identity Center.

AWS Directory Service memudahkan penyiapan dan menjalankan direktori di AWS Cloud, atau menghubungkan AWS sumber daya Anda dengan lokal Microsoft Active Directory yang ada. Setelah direktori Anda dibuat, Anda dapat menggunakannya untuk berbagai tugas:

- Mengelola pengguna dan grup
- Menyediakan sign-on tunggal ke aplikasi dan layanan
- Membuat dan menerapkan kebijakan grup
- Menyederhanakan penyebaran dan pengelolaan Linux berbasis cloud dan beban kerja Microsoft Windows
- Anda dapat menggunakan Microsoft AD AWS Terkelola untuk mengaktifkan otentikasi multi-faktor dengan mengintegrasikan dengan infrastruktur MFA berbasis Radio yang ada untuk menyediakan lapisan keamanan tambahan saat pengguna mengakses aplikasi AWS
- Terhubung dengan aman ke Amazon EC2 Linux dan instans Windows

> **Note**
>
> AWS mengelola lisensi instance Windows Server Anda untuk Anda; yang perlu Anda lakukan hanyalah membayar instans yang Anda gunakan. Juga tidak perlu membeli Lisensi Akses Klien Windows Server (CAL) tambahan, karena akses sudah termasuk dalam harga.

Setiap instans dilengkapi dengan dua koneksi remote untuk tujuan admin saja. Jika Anda memerlukan lebih dari dua koneksi, atau memerlukan koneksi tersebut untuk tujuan selain admin, Anda mungkin harus membawa CALs Layanan Desktop Jarak Jauh tambahan untuk digunakan di AWS.

Baca topik di bagian ini untuk mulai membuat direktori AD Microsoft AWS Terkelola, membuat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan direktori lokal, dan memperluas skema AD AWS Microsoft Terkelola.

Topik

- Memulai dengan Microsoft AD yang AWS Dikelola
- Konsep kunci untuk Microsoft AD yang Dikelola AWS
- Kasus penggunaan untuk Microsoft AD yang AWS Dikelola
- Cara mengelola Microsoft AD yang Dikelola AWS
- Praktik terbaik untuk Microsoft AD yang AWS Dikelola
- Kuota Microsoft AD yang Dikelola AWS
- Kompatibilitas aplikasi untuk Microsoft AD yang AWS Dikelola
- AWS Tutorial lab uji Microsoft AD yang dikelola
- Pemecahan Masalah AWS Microsoft AD yang Dikelola

Artikel blog AWS Keamanan Terkait

- Cara mendelegasikan administrasi direktori Microsoft AD AWS Terkelola ke pengguna Active Directory lokal
- Cara mengonfigurasi kebijakan kata sandi yang lebih kuat untuk membantu memenuhi standar keamanan Anda dengan menggunakan AWS Directory Service untuk Microsoft AD yang AWS Dikelola
- Cara meningkatkan redundansi dan kinerja Anda AWS Directory Service untuk AWS Microsoft AD yang Dikelola dengan menambahkan pengontrol Domain
- Cara mengaktifkan penggunaan desktop jarak jauh dengan menerapkan manajer lisensi desktop jarak jauh Microsoft di AWS Microsoft AD yang Dikelola
- Cara mengakses iklan Microsoft yang AWS Management ConsoleAWS Dikelola dan kredenal lokal Anda

- Cara mengaktifkan autentikasi multi-faktor untuk AWS layanan dengan menggunakan Managed AWS Microsoft AD dan kredensi lokal
- Cara mudah masuk ke AWS layanan dengan menggunakan Active Directory lokal

Memulai dengan Microsoft AD yang AWS Dikelola

AWS Microsoft AD yang dikelola membuat Microsoft Active Directory yang dikelola sepenuhnya di AWS Cloud dan didukung oleh Windows Server 2019 dan beroperasi pada tingkat fungsional R2 Forest dan Domain 2012. Saat Anda membuat direktori dengan Microsoft AD yang AWS Dikelola, AWS Directory Service buat dua pengontrol domain dan tambahkan layanan DNS atas nama Anda. Pengontrol domain dibuat dalam subnet yang berbeda di VPC Amazon, redundansi ini membantu memastikan bahwa direktori Anda tetap dapat diakses bahkan jika terjadi kegagalan. Jika Anda membutuhkan lebih banyak pengendali domain, Anda dapat menambahkannya nanti. Untuk informasi selengkapnya, lihat Men-deploy pengendali domain tambahan.

Topik

- AWS Prasyarat Microsoft AD yang dikelola
- Membuat iklan Microsoft AWS Terkelola Active Directory
- Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola
- Izin untuk akun Administrator

AWS Prasyarat Microsoft AD yang dikelola

Untuk membuat iklan Microsoft yang AWS DikelolaActive Directory, Anda memerlukan VPC Amazon dengan yang berikut ini:

- Setidaknya dua subnet. Setiap subnet harus berada di Availability Zone yang berbeda.
- VPC harus memiliki penghunian perangkat keras default.
- Anda tidak dapat membuat iklan Microsoft AWS Terkelola di VPC menggunakan alamat di ruang alamat 198.18.0.0/15.

Jika Anda perlu mengintegrasikan domain Microsoft AD AWS Terkelola dengan Active Directory domain lokal yang ada, Anda harus memiliki tingkat fungsional Forest dan Domain untuk domain lokal yang disetel ke Windows Server 2003 atau yang lebih tinggi.

AWS Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar AWS akun Anda, dan dikelola oleh. AWS Mereka memiliki dua adaptor jaringan, `ETH0` dan `ETH1`. `ETH0` adalah adaptor pengelola, dan berada di luar akun Anda. `ETH1` dibuat dalam akun Anda.

Rentang IP pengelola jaringan ETH0 direktori Anda adalah 198.18.0.0/15.

AWS IAM Identity Center prasyarat

Jika Anda berencana untuk menggunakan Pusat Identitas IAM dengan Microsoft AD yang AWS Dikelola, Anda perlu memastikan bahwa berikut ini benar:

- Direktori Microsoft AD AWS Terkelola Anda disiapkan di akun manajemen AWS organisasi Anda.
- Instance Pusat Identitas IAM Anda berada di Wilayah yang sama tempat direktori Microsoft AD AWS Terkelola Anda disiapkan.

Untuk informasi selengkapnya, lihat prasyarat Pusat Identitas IAM di Panduan Pengguna. AWS IAM Identity Center

Prasyarat autentikasi multi-faktor

Untuk mendukung autentikasi multi-faktor dengan direktori AWS Microsoft AD Terkelola, Anda harus mengonfigurasi server Layanan Pengguna Dial-In (RADIUS) Autentikasi Jarak Jauh (RADIUS) lokal atau berbasis Internet dengan cara berikut agar dapat menerima permintaan dari direktori Microsoft AD yang Dikelola di. AWS AWS

1. Di server RADIUS Anda, buat dua klien RADIUS untuk mewakili kedua pengontrol domain Microsoft AD AWS Terkelola (DC) di. AWS Anda harus mengkonfigurasi kedua klien menggunakan parameter umum berikut (server RADIUS Anda dapat bervariasi):
   - Alamat (DNS atau IP): Ini adalah alamat DNS untuk salah satu AWS Microsoft AD DC yang Dikelola. Kedua alamat DNS dapat ditemukan di AWS Directory Service Console pada halaman Detail direktori Microsoft AD yang AWS dikelola tempat Anda berencana untuk menggunakan MFA. Alamat DNS yang ditampilkan mewakili alamat IP untuk kedua DC AD Microsoft AWS Terkelola yang digunakan oleh. AWS

> **Note**
>
> Jika server RADIUS mendukung alamat DNS, Anda harus membuat hanya satu konfigurasi klien RADIUS. Jika tidak, Anda harus membuat satu konfigurasi klien RADIUS untuk setiap Microsoft AD DC yang Dikelola AWS .

- Angka port: Mengkonfigurasi nomor port yang server RADIUS Anda menerima koneksi klien RADIUS. Port RADIUS standar adalah 1812.
- Rahasia bersama: Ketik atau buat rahasia bersama yang server RADIUS akan gunakan untuk terhubung dengan klien RADIUS.
- Protokol: Anda mungkin perlu mengonfigurasi protokol otentikasi antara Microsoft AD DC yang AWS Dikelola dan server RADIUS. Protokol yang didukung adalah PAP, CHAP MS-CHAPv1, dan MS-CHAPv2. MS-CHAPv2 direkomendasikan karena menyediakan keamanan terkuat dari tiga pilihan.
- Nama aplikasi: Ini mungkin opsional di beberapa server RADIUS dan biasanya mengidentifikasi aplikasi dalam pesan atau laporan.

2. Konfigurasikan jaringan yang ada untuk mengizinkan lalu lintas masuk dari klien RADIUS (Alamat DNS Microsoft AD DC yang AWS dikelola, lihat Langkah 1) ke port server RADIUS Anda.
3. Tambahkan aturan ke grup keamanan Amazon EC2 di domain AWS Microsoft AD Terkelola yang memungkinkan lalu lintas masuk dari alamat DNS server RADIUS dan nomor port yang ditentukan sebelumnya. Untuk informasi selengkapnya, lihat Menambahkan aturan ke sebuah grup keamanan di Panduan Pengguna EC2.

Untuk informasi selengkapnya tentang menggunakan Microsoft AD yang AWS Dikelola dengan MFA, lihat. Mengaktifkan autentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS

Membuat iklan Microsoft AWS Terkelola Active Directory

Untuk membuat direktori baru, lakukan langkah-langkah berikut. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan prasyarat yang diidentifikasi dalam AWS Prasyarat Microsoft AD yang dikelola.

Untuk membuat direktori Microsoft AD yang AWS Dikelola

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih Microsoft AD yang Dikelola AWS , lalu pilih Selanjutnya.

3. Di halaman Masukkan informasi direktori, berikan informasi berikut:

   Edisi

   Pilih dari Edisi Standar atau Edisi Perusahaan dari Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya tentang edisi, lihat Directory Service AWS untuk Microsoft Active Directory.

   Nama Sistem Nama Domain Direktori (DNS)

   Nama berkualifikasi penuh untuk direktori, seperti `corp.example.com`.

   > **Note**
   >
   > Jika Anda berencana menggunakan Amazon Route 53 untuk DNS, nama domain Microsoft AD yang AWS Dikelola harus berbeda dengan nama domain Route 53 Anda. Masalah resolusi DNS dapat terjadi jika Route 53 dan Microsoft AD yang AWS Dikelola berbagi nama domain yang sama.

   Direktori nama NetBIOS

   Nama singkat untuk direktori, seperti `CORP`.

   Deskripsi direktori

   Deskripsi opsional untuk direktori.

   Kata sandi admin

   Kata sandi administrator direktori. Proses pembuatan direktori menciptakan akun administrator dengan nama pengguna `Admin` dan kata sandi ini.

   Kata sandi tidak dapat menyertakan kata "admin."

   Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

   - Huruf kecil (a-z)
   - Huruf besar (A-Z)
   - Angka (0-9)

- Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Konfirmasikan kata sandi

Ketik ulang kata sandi administrator.

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

   VPC

   VPC untuk direktori.

   Subnet

   Pilih subnet untuk pengendali domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.

5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Membuat direktori membutuhkan waktu 20 sampai 40 menit. Setelah dibuat, nilai Status berubah ke Aktif.

Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola

Saat Anda membuat Direktori Aktif dengan Microsoft AD yang AWS Dikelola, AWS Directory Service lakukan tugas berikut atas nama Anda:

- Secara otomatis membuat dan mengasosiasikan antarmuka jaringan elastis (ENI) dengan masing-masing pengendali domain Anda. Masing-masing ENI ini penting untuk konektivitas antara VPC AWS Directory Service dan pengontrol domain Anda dan tidak boleh dihapus. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan AWS Directory Service dengan deskripsi: "AWS menciptakan antarmuka jaringan untuk direktori-id direktori". Untuk informasi selengkapnya, lihat Antarmuka Jaringan Elastis di Panduan Pengguna Amazon EC2 untuk Instans Windows. Server DNS default dari Microsoft AD yang AWS Dikelola Active Directory adalah server DNS VPC di Classless Inter-Domain Routing (CIDR) +2. Untuk informasi selengkapnya, lihat Server DNS Amazon di Panduan Pengguna Amazon VPC.

> **Note**
>
> Pengontrol domain diterapkan di dua Availability Zone di suatu wilayah secara default dan terhubung ke Amazon VPC (VPC) Anda. Pencadangan diambil secara otomatis sekali sehari, dan volume Amazon EBS (EBS) dienkripsi untuk memastikan bahwa data

diamankan saat istirahat. Pengendali domain yang gagal secara otomatis diganti di Availability Zone yang sama menggunakan alamat IP yang sama, dan pemulihan bencana penuh dapat dilakukan dengan menggunakan backup terbaru.

- Persediaan Direktori Aktif dalam VPC Anda menggunakan dua pengendali domain untuk toleransi kesalahan dan ketersediaan tinggi. Pengendali domain yang lebih dapat disediakan untuk ketahanan yang lebih tinggi dan performa setelah direktori telah berhasil dibuat dan Aktif. Untuk informasi selengkapnya, lihat Men-deploy pengendali domain tambahan.

  > **Note**
  >
  > AWS tidak mengizinkan penginstalan agen pemantauan pada pengontrol domain Microsoft AD AWS Terkelola.

- Membuat AWS kelompok keamanan yang menetapkan aturan jaringan untuk lalu lintas masuk dan keluar dari pengendali domain Anda. Aturan keluar default mengizinkan semua ENI lalu lintas atau instance yang dilampirkan ke Grup Keamanan yang dibuat. AWS Aturan masuk default hanya mengizinkan lalu lintas melalui port-port yang diperlukan oleh Direktori Aktif dari setiap sumber (0.0.0.0/0). Aturan 0.0.0.0/0 tidak memperkenalkan kerentanan keamanan karena lalu lintas ke pengontrol domain terbatas pada lalu lintas dari VPC Anda, dari VPC peered lainnya, atau dari jaringan yang telah Anda sambungkan menggunakan, Transit Gateway, atau Jaringan Pribadi Virtual. AWS Direct Connect AWS Untuk keamanan tambahan, ENI yang dibuat tidak memiliki IP Elastis melekat padanya dan Anda tidak memiliki izin untuk melampirkan IP Elastis untuk ENI tersebut. Oleh karena itu, satu-satunya lalu lintas masuk yang dapat berkomunikasi dengan Microsoft AD AWS Terkelola Anda adalah lalu lintas lokal yang dirutekan VPC dan VPC. Gunakan sangat hati-hati jika Anda mencoba untuk mengubah aturan-aturan ini karena mungkin dapat merusak kemampuan Anda untuk berkomunikasi dengan pengendali domain Anda. Untuk informasi selengkapnya, lihat Praktik terbaik untuk Microsoft AD yang AWS Dikelola. Aturan Grup AWS Keamanan berikut dibuat secara default:

  Aturan Masuk

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
ICMP	N/A	0.0.0.0/0	Ping	LDAP Tetap Hidup, DFS

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	0.0.0.0/0	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	0.0.0.0/0	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	0.0.0.0/0	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP & UDP	445	0.0.0.0/0	SMB / CIFS	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP & UDP	464	0.0.0.0/0	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentikasi komputer, kepercayaan
TCP	135	0.0.0.0/0	Replikasi	RPC, EPM

Protokol	Rentang port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	636	0.0.0.0/0	LDAP SSL	Direktori , replikasi , pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP	1024 - 65535	0.0.0.0/0	RPC	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	0.0.0.0/0	LDAP GC & LDAP GC SSL	Direktori , replikasi , pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
UDP	123	0.0.0.0/0	Waktu Windows	Waktu Windows, kepercayaan
UDP	138	0.0.0.0/0	DFSN & NetLogon	DFS, kebijakan grup
Semua	Semua	sg-###### ########	Semua Lalu Lintas	

Aturan Keluar

Protokol	Rentang Port	Tujuan	Jenis lalu lintas	Penggunaan Direktori Aktif
Semua	Semua	sg-###### ########	Semua Lalu Lintas	

- Untuk informasi selengkapnya tentang port dan protokol yang digunakan oleh Active Directory, lihat Ringkasan layanan dan persyaratan port jaringan untuk Windows di dokumentasi Microsoft.
- Membuat akun administrator direktori dengan nama pengguna Admin dan kata sandi yang ditentukan. Akun ini terletak di bawah Pengguna OU (Contohnya, Corp > Pengguna). Anda menggunakan akun ini untuk mengelola direktori Anda di AWS Cloud. Untuk informasi selengkapnya, lihat Izin untuk akun Administrator.

> **Important**
>
> Pastikan untuk menyimpan kata sandi ini. AWS Directory Service tidak menyimpan kata sandi ini, dan tidak dapat diambil. Namun, Anda dapat mengatur ulang kata sandi dari AWS Directory Service konsol atau dengan menggunakan ResetUserPasswordAPI.

- Menciptakan tiga unit organisasi (OUs) berikut di bawah root domain:

Nama OU	Deskripsi
AWS Grup yang Delegasikan	Menyimpan semua grup yang dapat Anda gunakan untuk mendelegasikan izin AWS tertentu kepada pengguna Anda.
AWS Dilindungi	Menyimpan semua akun khusus AWS manajemen.
<yourdomainname>	Nama OU ini didasarkan dari nama NetBIOS yang Anda ketik saat membuat direktori. Jika Anda tidak menentukan nama NetBIOS, nama itu akan default ke bagian pertama dari nama DNS direktori Anda (misalnya, dalam kasus corp.example.com, nama NetBIOS adalah corp). OU ini dimiliki oleh AWS dan berisi

Nama OU	Deskripsi

	semua objek direktori AWS terkait Anda, yang Anda diberikan Kontrol Penuh atas. Dua anak OU ada di bawah OU ini secara default; Komputer dan Pengguna. Sebagai contoh:
	• Corp
	  • Komputer
	  • Pengguna

- Membuat grup berikut di Grup AWS Delegasi OU:

Nama grup	Deskripsi
AWS Operator Akun yang Delegasikan	Anggota grup keamanan ini memiliki kemampuan manajemen akun terbatas seperti pengaturan ulang kata sandi
AWS Administrator Aktivasi Berbasis Direktori Aktif yang Delegasikan	Anggota grup keamanan ini dapat membuat objek aktivasi lisensi volume Directory Aktif, yang memungkinkan korporasi untuk mengaktifkan komputer melalui sambungan ke domain mereka.
AWS Delegasikan Tambahkan Workstation Ke Pengguna Domain	Anggota grup keamanan ini dapat menggabun gkan 10 komputer ke sebuah domain.
AWS Administrator yang didelegasikan	Anggota grup keamanan ini dapat mengelola Microsoft AD yang AWS Dikelola, memiliki kontrol penuh atas semua objek di OU Anda dan dapat mengelola grup yang terdapat dalam OU Grup AWS Delegasi.
AWS Delegasi Diizinkan untuk Mengauten tikasi Objek	Anggota grup keamanan ini diberikan kemampuan untuk mengautentikasi ke sumber daya komputer di OU AWS Cadangan

Nama grup	Deskripsi
	(Hanya diperlukan untuk objek lokal dengan Trusts yang diaktifkan Autentikasi Selektif).
AWS Delegasi Diizinkan untuk Mengauten tikasi ke Pengontrol Domain	Anggota grup keamanan ini diberikan kemampuan untuk mengautentikasi ke sumber daya komputer di Pengendali Domain OU (hanya diperlukan untuk objek on-promise dengan Kepercayaan yang Autentikasi Selektif diaktifkan).
AWS Administrator Seumur Hidup Objek Dihapus yang Delegasikan	Anggota grup keamanan ini dapat memodifik asi DeletedObjectLifetime objek MSDS-, yang menentukan berapa lama objek yang dihapus akan tersedia untuk dipulihkan dari Tempat Sampah AD.
AWS Administrator Sistem File Terdistribusi yang Delegasikan	Anggota grup keamanan ini dapat menambah dan menghapus FRS, DFS-R, dan ruang nama DFS.
AWS Administrator Sistem Nama Domain yang Delegasikan	Anggota grup keamanan ini dapat mengelola DNS terintegrasi Direktori Aktif.
AWS Administrator Protokol Konfigurasi Host Dinamis yang Delegasikan	Anggota grup keamanan ini dapat mengautor isasi server Windows DHCP di korporasi.
AWS Administrator Otoritas Sertifikat Perusahaan yang Delegasikan	Anggota grup keamanan ini dapat men-deploy dan mengelola infrastruktur Otoritas Sertifikat Microsoft Enterprise.
AWS Administrator Kebijakan Kata Sandi Berbutir Halus yang Delegasikan	Anggota grup keamanan ini dapat memodifik asi kebijakan kata sandi terperinci yang telah dibuat sebelumnya.
AWS Administrator FSx yang didelegasikan	Anggota grup keamanan ini diberikan kemampuan untuk mengelola sumber daya Amazon FSx.

Nama grup	Deskripsi
AWS Administrator Kebijakan Grup yang Delegasikan	Anggota grup keamanan ini dapat melakukan tugas manajemen kebijakan grup (membuat, mengedit, menghapus, tautan).
AWS Administrator Delegasi Kerberos yang Delegasi	Anggota grup keamanan ini dapat mengaktif kan delegasi pada komputer dan objek akun pengguna.
AWS Administrator Akun Layanan Terkelola yang Delegasikan	Anggota grup keamanan ini dapat membuat dan menghapus Akun Layanan Terkelola.
AWS Perangkat Non-Compliant MS-NPRC yang Delegasikan	Anggota grup keamanan ini akan diberikan pengecualian dari memerlukan komunikas i saluran aman dengan pengendali domain. Grup ini adalah untuk akun komputer.
AWS Administrator Layanan Akses Jarak Jauh yang Delegasikan	Anggota grup keamanan ini dapat menambah dan menghapus server RAS dari grup Server RAS dan IAS.
AWS Administrator Perubahan Direktori Replikasi yang Delegasikan	Anggota grup keamanan ini dapat menyinkro nkan informasi profil di Active Directory dengan SharePoint Server.
AWS Administrator Server yang Delegasikan	Anggota grup keamanan ini termasuk dalam grup administrator lokal pada semua komputer yang tergabung di domain.
AWS Administrator Situs dan Layanan yang Delegasikan	Anggota grup keamanan ini dapat mengubah nama objek Default-First-Site-Name di Situs dan Layanan Direktori Aktif.
AWS Administrator Manajemen Sistem yang Delegasikan	Anggota grup keamanan ini dapat membuat dan mengelola objek dalam kontainer pengelolaan sistem.

Nama grup	Deskripsi
AWS Administrator Lisensi Server Terminal yang Delegasikan	Anggota grup keamanan ini dapat menambah dan menghapus Server Lisensi Server Terminal dari grup Server Lisensi Server Terminal.
AWS Administrator Akhiran Nama Utama Pengguna yang Delegasikan	Anggota grup keamanan ini dapat menambah dan menghapus akhiran nama utama pengguna.

- Menciptakan dan menerapkan Objek Kebijakan Grup (GPO) berikut:

> **Note**
>
> Anda tidak memiliki izin untuk menghapus, memodifikasi, atau membatalkan tautan GPO ini. Ini dengan desain karena dicadangkan untuk AWS digunakan. Anda dapat menautkan mereka ke OU yang Anda kendalikan jika diperlukan.

Nama kebijakan grup	Berlaku untuk	Deskripsi
Kebijakan Domain Default	Domain	Termasuk kebijakan kata sandi domain dan Kerberos.
ServerAdmins	Semua akun komputer pengendali non domain	Menambahkan 'Administ rator Server AWS Delegasi' sebagai anggota Grup BUILTIN\ Administrators.
AWS Kebijakan Cadangan: Pengguna	AWS Akun pengguna yang dicadangkan	Menetapkan pengaturan keamanan yang disarankan pada semua akun pengguna di OU AWS Cadangan.
AWS Kebijakan Direktori Aktif Terkelola	Semua pengendali domain	Atur pengaturan keamanan yang direkomendasikan pada semua pengendali domain.

Nama kebijakan grup	Berlaku untuk	Deskripsi
TimePolicyNT5DS	Semua pengendali domain non PDCe	Atur semua kebijakan waktu pengendali domain non PDCe untuk menggunakan Windows Time (NT5DS).
TimePolicyPDC	Pengendali domain PDCe	Atur kebijakan waktu pengendali domain PDCe untuk menggunakan Network Time Protocol (NTP).
Kebijakan pengendali Domain default	Tidak digunakan	Disediakan selama pembuatan domain, Kebijakan Direktori Aktif AWS Terkelola digunakan sebagai gantinya.

Jika Anda ingin melihat pengaturan dari setiap GPO, Anda dapat melihat mereka dari instans Windows yang tergabung domain misalnya dengan Konsol Manajemen kebijakan grup (GPMC)diaktifkan.

Izin untuk akun Administrator

Saat Anda membuat AWS direktori Directory Service untuk Microsoft Active Directory, AWS buat unit organisasi (OU) untuk menyimpan semua grup dan akun AWS terkait. Untuk informasi selengkapnya tentang OU ini, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola. Ini termasuk akun Admin. Akun Admin memiliki izin untuk melakukan aktivitas administratif umum berikut untuk OU Anda:

- Menambahkan, memperbarui, atau menghapus pengguna, grup, dan komputer. Untuk informasi selengkapnya, lihat Mengelola pengguna dan grup di Microsoft AD yang Dikelola AWS.
- Menambahkan sumber daya ke domain Anda seperti server file atau cetak, kemudian berikan izin untuk sumber daya tersebut ke pengguna dan grup di OU Anda.
- Buat OU dan kontainer tambahan.

- Otoritas delegasi dari OUs dan kontainer tambahan. Untuk informasi selengkapnya, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.
- Membuat dan menautkan kebijakan grup.
- Memulihkan objek yang dihapus dari Keranjang Sampah Directory Active.
- Jalankan Windows PowerShell modul Active Directory dan DNS di Active Directory Web Service.
- Buat dan konfigurasi Akun Layanan Terkelola grup. Untuk informasi selengkapnya, lihat Akun Layanan yang Dikelola Grup.
- Mengkonfigurasi delegasi terbatas Kerberos. Untuk informasi selengkapnya, lihat Delegasi terbatas Kerberos.

Akun Admin juga memiliki hak untuk melakukan aktivitas di seluruh domain berikut:

- Mengelola konfigurasi DNS (menambahkan, menghapus, atau memperbarui catatan, zona, dan penerus)
- Melihat log peristiwa DNS
- Melihat log peristiwa keamanan

Hanya tindakan yang tercantum di sini yang diizinkan untuk akun Admin. Akun Admin juga tidak memiliki izin untuk setiap tindakan terkait direktori di luar OU spesifik Anda, seperti pada OU induk.

Important

AWS Administrator Domain memiliki akses administratif penuh ke semua domain yang di-host. AWS Lihat perjanjian Anda AWS dan FAQ perlindungan AWS data untuk informasi selengkapnya tentang cara AWS menangani konten, termasuk informasi direktori, yang Anda simpan di AWS sistem.

Note

Kami merekomendasikan agar Anda tidak menghapus atau mengubah nama akun ini. Jika Anda tidak lagi ingin menggunakan akun, kami sarankan Anda menetapkan kata sandi yang panjang (paling banyak 64 karakter acak) dan kemudian nonaktifkan akun.

Akun istimewa administrator korporasi dan domain

AWS secara otomatis memutar kata sandi Administrator bawaan ke kata sandi acak setiap 90 hari. Kapan saja kata sandi Administrator bawaan diminta untuk penggunaan manusia, AWS tiket dibuat dan dicatat dengan AWS Directory Service tim. Kredensial akun dienkripsi dan ditangani melalui saluran aman. Juga kredensi akun Administrator hanya dapat diminta oleh tim AWS Directory Service manajemen.

Untuk melakukan manajemen operasional direktori Anda, AWS memiliki kontrol eksklusif atas akun dengan hak istimewa Administrator Perusahaan dan Administrator Domain. Ini termasuk kontrol eksklusif akun administrator Direktori Aktif. AWS melindungi akun ini dengan mengotomatiskan manajemen kata sandi melalui penggunaan brankas kata sandi. Selama rotasi otomatis kata sandi administrator, AWS buat akun pengguna sementara dan berikan hak istimewa Administrator Domain. Akun sementara ini digunakan sebagai back-up jika terjadi kegagalan rotasi kata sandi pada akun administrator. Setelah AWS berhasil memutar kata sandi administrator, AWS menghapus akun administrator sementara.

Biasanya AWS mengoperasikan direktori sepenuhnya melalui otomatisasi. Jika proses otomatisasi tidak dapat menyelesaikan masalah operasional, AWS mungkin perlu meminta insinyur dukungan masuk ke pengontrol domain (DC) Anda untuk melakukan diagnosis. Dalam kasus yang jarang terjadi ini, AWS menerapkan sistem permintaan/pemberitahuan untuk memberikan akses. Dalam proses ini, AWS otomatisasi membuat akun pengguna terbatas waktu di direktori Anda yang memiliki izin Administrator Domain. AWS mengaitkan akun pengguna dengan insinyur yang ditugaskan untuk bekerja di direktori Anda. AWS mencatat asosiasi ini dalam sistem log kami dan memberikan insinyur dengan kredensi untuk digunakan. Semua tindakan yang diambil oleh teknisi dicatat dalam log peristiwa Windows. Ketika waktu yang dialokasikan berlalu, otomatisasi menghapus akun pengguna.

Anda dapat memantau tindakan akun administratif dengan menggunakan fitur penerusan log direktori Anda. Fitur ini memungkinkan Anda untuk meneruskan peristiwa Keamanan AD ke CloudWatch sistem Anda di mana Anda dapat menerapkan solusi pemantauan. Untuk informasi selengkapnya, lihat Mengaktifkan penerusan log.

ID Peristiwa Keamanan 4624, 4672 dan 4648 semua dicatat ketika seseorang log ke DC secara interaktif. Anda dapat melihat setiap log peristiwa Keamanan Windows DC menggunakan Event Viewer Microsoft Management Console (MMC) dari komputer Windows yang digabungkan dengan domain. Anda juga dapat Mengaktifkan penerusan log mengirim semua log peristiwa Keamanan ke CloudWatch Log di akun Anda.

Anda mungkin sesekali melihat pengguna yang dibuat dan dihapus dalam OU AWS Cadangan. AWS bertanggung jawab atas pengelolaan dan keamanan semua objek di OU ini dan OU atau wadah lainnya di mana kami belum mendelegasikan izin bagi Anda untuk mengakses dan mengelola. Anda mungkin melihat pembuatan dan penghapusan di OU tersebut. Ini karena AWS Directory Service menggunakan otomatisasi untuk memutar kata sandi Administrator Domain secara teratur. Ketika kata sandi dirotasi, backup dibuat pada peristiwa rotasi yang gagal. Setelah rotasi berhasil, akun backup akan dihapus secara otomatis. Juga dalam hal langka bahwa akses interaktif diperlukan pada DC untuk tujuan pemecahan masalah, akun pengguna sementara dibuat untuk digunakan oleh seorang AWS Directory Service insinyur. Setelah teknisi menyelesaikan pekerjaan mereka, akun pengguna sementara akan dihapus. Perhatikan bahwa setiap kali kredensil interaktif diminta untuk direktori, tim AWS Directory Service manajemen akan diberi tahu.

Konsep kunci untuk Microsoft AD yang Dikelola AWS

Anda akan mendapatkan lebih banyak dari Microsoft AD yang Dikelola AWS jika Anda terbiasa dengan konsep-konsep kunci berikut.

Topik

Skema Direktori Aktif

Skema adalah definisi atribut dan kelas yang merupakan bagian dari direktori terdistribusi dan mirip dengan bidang dan tabel dalam basis data. Skema termasuk seperangkat aturan yang menentukan jenis dan format data yang dapat ditambahkan atau disertakan dalam basis data. Kelas Pengguna adalah salah satu contoh dari kelas yang disimpan dalam basis data. Beberapa contoh dari atribut kelas Pengguna dapat mencakup nama depan pengguna, nama belakang, nomor telepon, dan sebagainya.

Elemen skema

Atribut, kelas dan objek adalah elemen dasar yang digunakan untuk membangun definisi objek dalam skema. Hal berikut ini memberikan detail tentang elemen skema yang penting untuk diketahui sebelum Anda memulai proses untuk memperpanjang skema Microsoft AD yang Dikelola AWS Anda.

Atribut

Setiap atribut skema, yang mirip dengan bidang dalam basis data, memiliki beberapa properti yang menentukan karakteristik atribut. Misalnya, properti yang digunakan oleh klien LDAP untuk membaca dan menulis atribut `LDAPDisplayName`. Properti `LDAPDisplayName` harus unik di semua atribut dan kelas. Untuk daftar lengkap karakteristik atribut, lihat Karakteristik Atribut pada situs web MSDN. Untuk pedoman tambahan tentang cara membuat atribut baru, lihat Menentukan Atribut Baru pada situs web MSDN.

Kelas

Kelas-kelas adalah analog dengan tabel dalam database dan juga memiliki beberapa sifat untuk ditentukan. Misalnya, `objectClassCategory` menentukan kategori kelas. Untuk daftar lengkap karakteristik atribut, lihat Karakteristik Atribut pada situs web MSDN. Untuk informasi selengkapnya tentang cara membuat kelas baru, lihat Menentukan Kelas Baru pada situs web MSDN.

Pengenal objek (OID)

Setiap kelas dan atribut harus memiliki OID yang unik untuk semua objek Anda. Vendor perangkat lunak harus mendapatkan OID mereka sendiri untuk memastikan keunikan. Keunikan menghindari konflik ketika atribut yang sama digunakan oleh lebih dari satu aplikasi untuk tujuan yang berbeda. Untuk memastikan keunikan, Anda dapat memperoleh OID root dari Otoritas Pendaftaran Nama ISO. Atau, Anda dapat memperoleh dasar OID dari Microsoft. Untuk informasi selengkapnya tentang OID dan cara mendapatkannya, lihat Pengidentifikasi objek pada situs web MSDN.

Atribut terkait skema

Beberapa atribut dihubungkan antara dua kelas dengan tautan terusan dan kembali. Contoh terbaik adalah grup Ketika Anda melihat grup itu menunjukkan kepada Anda anggota grup; jika Anda melihat pengguna Anda dapat melihat grup apa yang menjadi miliknya. Ketika Anda menambahkan pengguna ke grup, Direktori Aktif membuat tautan terusan ke grup. Kemudian Direktori Aktif menambahkan tautan kembali dari grup ke pengguna. ID tautan unik harus dibuat saat membuat atribut yang akan ditautkan. Untuk informasi selengkapnya, lihat Atribut Tertaut pada situs web MSDN.

Topik terkait

- Kapan harus memperpanjang skema Microsoft AD yang Dikelola AWS Anda
- Tutorial: Memperluas skema AD Microsoft yang AWS Dikelola

Patching dan pemeliharaan Microsoft AD yang Dikelola AWS

Directory Service untuk Microsoft Active Directory AWS, juga dikenal sebagai DS AWS untuk Microsoft AD yang Dikelola AWS, sebenarnya merupakan Microsoft Active Directory Domain Services (AD DS), disampaikan sebagai layanan terkelola. Sistem ini menggunakan Microsoft Windows Server 2019 untuk pengontrol domain (DC), dan AWS menambahkan perangkat lunak ke DC untuk tujuan manajemen layanan. AWSpembaruan (tambalan) DC untuk menambahkan fungsionalitas baru dan menjaga perangkat lunak Microsoft Windows Server tetap terkini. Selama proses patch, direktori Anda tetap tersedia untuk digunakan.

Memastikan ketersediaan

Secara default setiap direktori terdiri dari dua DC, masing-masing diinstal di Availability Zone yang berbeda. Sesuai pilihan Anda, Anda dapat menambahkan DC untuk lebih meningkatkan ketersediaan. Untuk lingkungan kritis yang membutuhkan ketersediaan tinggi dan toleransi kesalahan, sebaiknya gunakan DC tambahan. AWSmenambal DC Anda secara berurutan, selama waktu itu DC yang secara aktif menambal AWS tidak tersedia. Jika satu atau lebih DC Anda tidak berfungsi sementara, AWS menunda patching sampai direktori Anda memiliki setidaknya dua DC operasional. Hal ini memungkinkan Anda menggunakan DC operasi lain selama proses patch, yang biasanya memakan waktu 30 sampai 45 menit per DC, meskipun kali ini dapat bervariasi. Untuk memastikan aplikasi Anda dapat mencapai operasi DC jika satu atau lebih DC tidak tersedia untuk alasan apapun, termasuk mem-patch, aplikasi Anda harus menggunakan layanan locator Windows DC dan tidak menggunakan alamat DC statis.

Memahami jadwal patching

Untuk menjaga perangkat lunak Microsoft Windows Server saat ini pada DC Anda, AWS memanfaatkan pembaruan Microsoft. Karena Microsoft membuat patch rollup bulanan tersedia untuk Windows Server, AWS membuat upaya terbaik untuk menguji dan menerapkan rollup untuk semua DC pelanggan dalam waktu tiga minggu kalender. Selain itu, AWS meninjau pembaruan yang dirilis Microsoft di luar rollup bulanan berdasarkan penerapan untuk DC dan urgensi. Untuk patch keamanan yang Microsoft nilai sebagai Kritis atau Penting, dan yang relevan dengan DC, AWS melakukan segala upaya untuk menguji dan men-deploy patch dalam waktu lima hari.

Akun Layanan yang Dikelola Grup

Dengan Windows Server 2012, Microsoft memperkenalkan metode baru yang dapat digunakan administrator untuk mengelola akun layanan yang disebut Akun Layanan yang Dikelola grup

(gMSAs). Menggunakan gMSAs, administrator layanan tidak lagi diperlukan untuk secara manual mengelola sandi sinkronisasi antara instans layanan. Sebaliknya, administrator hanya dapat membuat gMSA di Direktori Aktif dan kemudian mengkonfigurasi beberapa instans layanan untuk menggunakan gMSA tunggal.

Untuk memberikan izin sehingga pengguna di Microsoft AD yang Dikelola AWS dapat membuat gMSA, Anda harus menambahkan akun mereka sebagai anggota dari grup keamanan Administrator Akun Layanan Terkelola yang Didelegasikan AWS. Secara default, akun Admin adalah anggota grup ini. Untuk informasi selengkapnya tentang GMSA, lihat Ringkasan Akun Layanan Terkelola Grup di situs web Microsoft. TechNet

Posting Blog AWS Keamanan Terkait

- Bagaimana Microsoft AD yang AWS Dikelola Membantu Menyederhanakan Penerapan dan Meningkatkan Keamanan Direktori Aktif — Aplikasi .NET Terintegrasi

Delegasi terbatas Kerberos

Kerberos constrained delegation adalah sebuah fitur di Windows Server. Fitur ini memberikan administrator layanan untuk menentukan dan memberlakukkan batasan kepercayaan aplikasi dengan membatasi lingkup tempat layanan aplikasi dapat bertindak atas nama pengguna. Hal ini dapat berguna ketika Anda perlu mengkonfigurasi akun layanan front-end yang dapat mendelegasikan ke layanan backend mereka. Kerberos constrained delegation juga mencegah gMSA Anda untuk menghubungkan ke setiap dan semua layanan atas nama pengguna Direktori Aktif Anda, menghindari potensi penyalahgunaan oleh developer nakal.

Sebagai contoh, katakanlah pengguna jsmith masuk ke aplikasi HR. Anda ingin SQL Server untuk menerapkan izin basis data jsmith. Namun, secara default SQL Server membuka koneksi database menggunakan kredensyal akun layanan yang menerapkan hr-app-service izin alih-alih izin yang dikonfigurasi jsmith. Anda harus membuatnya mungkin untuk aplikasi HR penggajian untuk mengakses basis data SQL Server menggunakan kredensial jsmith. Untuk melakukannya, Anda mengaktifkan delegasi terbatas Kerberos untuk akun hr-app-service layanan di direktori AWS Microsoft AD Terkelola di. AWS Ketika jsmith masuk, Direktori Aktif menyediakan tiket Kerberos yang secara otomatis Windows gunakan ketika jsmith mencoba untuk mengakses layanan lain dalam jaringan. Delegasi Kerberos memungkinkan hr-app-service akun untuk menggunakan kembali tiket jsmith Kerberos saat mengakses database, sehingga menerapkan izin khusus untuk jsmith saat membuka koneksi database.

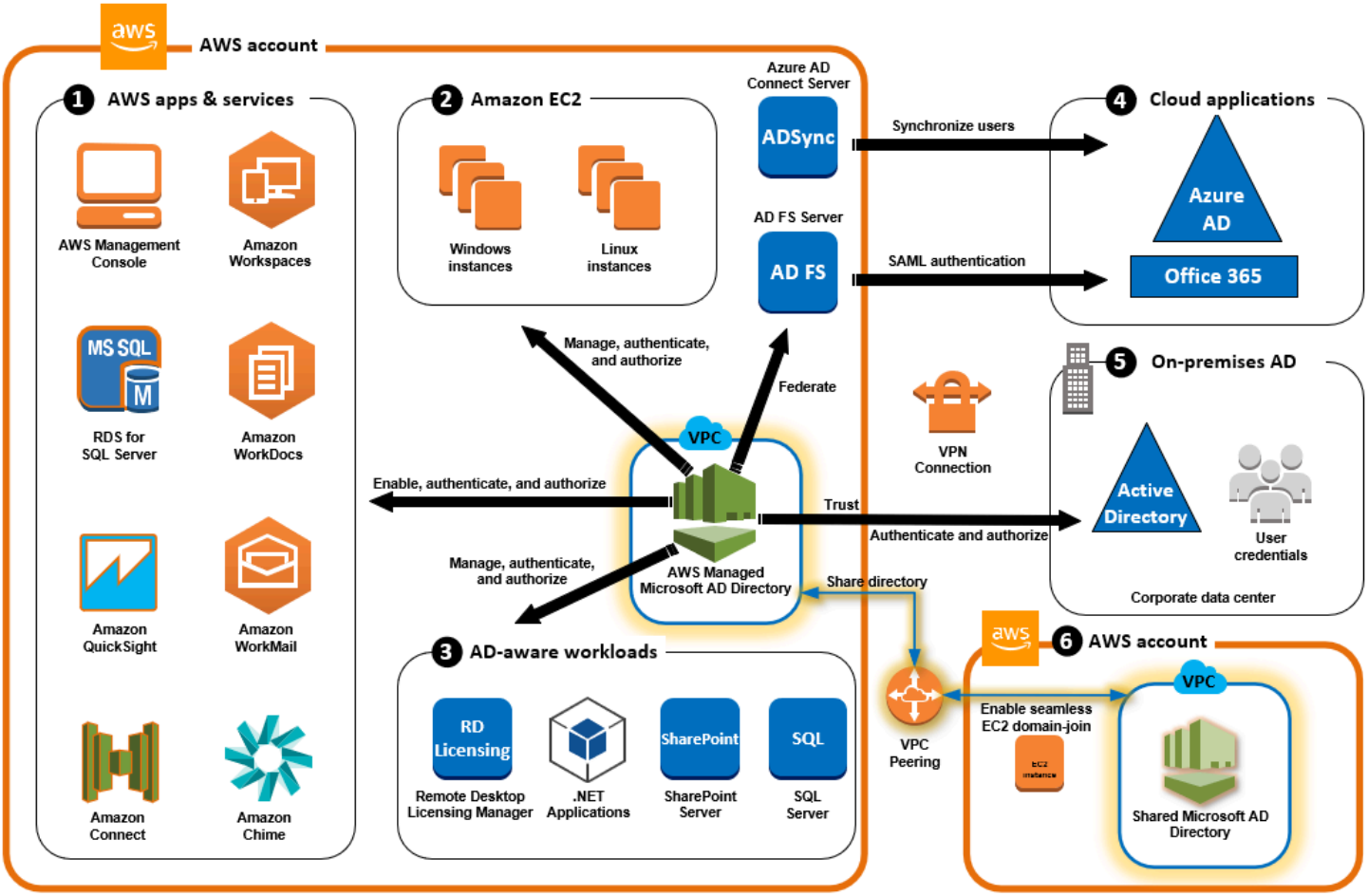
Untuk memberikan izin yang memungkinkan pengguna di Microsoft AD yang Dikelola AWS untuk mengkonfigurasi delegasi terbatas Kerberos, Anda harus menambahkan akun mereka sebagai anggota dari grup keamanan Administrator Delegasi Kerberos yang Didelegasikan AWS. Secara default, akun Admin adalah anggota grup ini. Untuk informasi selengkapnya tentang delegasi terbatas Kerberos, lihat Ikhtisar Delegasi Terbatas Kerberos di situs web Microsoft. TechNet

Delegasi terbatas berbasis sumber daya diperkenalkan dengan Windows Server 2012. Ini menyediakan layanan back-end administrator kemampuan untuk mengkonfigurasi delegasi terbatas untuk layanan.

Kasus penggunaan untuk Microsoft AD yang AWS Dikelola

Dengan Microsoft AD yang AWS Dikelola, Anda dapat berbagi satu direktori untuk beberapa kasus penggunaan. Misalnya, Anda dapat berbagi direktori untuk mengautentikasi dan mengotorisasi akses untuk aplikasi .NET, Amazon RDS for SQL Server dengan Autentikasi Windows diaktifkan, dan Amazon Chime untuk olahpesan dan konferensi video.

Diagram berikut menunjukkan beberapa kasus penggunaan untuk direktori Microsoft AD AWS Terkelola Anda. Ini termasuk kemampuan untuk memberikan pengguna Anda akses ke aplikasi cloud eksternal dan memungkinkan pengguna Active Directory lokal untuk mengelola dan memiliki akses ke sumber daya di AWS Cloud.



Gunakan Microsoft AD yang AWS Dikelola untuk salah satu kasus penggunaan bisnis berikut.

Topik

- Kasus Penggunaan 1: Masuk ke AWS aplikasi dan layanan dengan kredensyal Active Directory
- Kasus Penggunaan 2: Mengelola instans Amazon EC2
- Kasus Penggunaan 3: Menyediakan layanan direktori ke beban kerja yang sadar Direktori Aktif
- Kasus Penggunaan 4: AWS IAM Identity Center ke Office 365 dan aplikasi cloud lainnya
- Kasus Penggunaan 5: Memperluas Direktori Aktif lokal Anda ke Cloud AWS
- Kasus Penggunaan 6: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh akun AWS

Kasus Penggunaan 1: Masuk ke AWS aplikasi dan layanan dengan kredensyal Active Directory

Anda dapat mengaktifkan beberapa AWS aplikasi dan layanan seperti AWS Client VPN,, Amazon Chime AWS Management ConsoleAWS IAM Identity Center, Amazon Connect, Amazon FSx, Amazon, Amazon, QuickSightAmazon RDS for SQL WorkDocs Server, Amazon, Amazon, WorkMail Amazon WorkSpaces, AWS dan menggunakan direktori AD Microsoft Terkelola Anda. Ketika Anda mengaktifkan AWS aplikasi atau layanan di direktori Anda, pengguna Anda dapat mengakses aplikasi atau layanan dengan kredensi Direktori Aktif mereka.

Misalnya, Anda dapat mengaktifkan pengguna Anda untuk masuk AWS Management Console dengan kredensyal Direktori Aktif mereka. Untuk melakukan ini, Anda mengaktifkan AWS Management Console sebagai aplikasi di direktori Anda, dan kemudian menetapkan pengguna dan grup Direktori Aktif Anda ke peran IAM. Saat pengguna Anda masuk ke AWS Management Console, mereka mengambil peran IAM untuk mengelola AWS sumber daya. Hal ini memudahkan Anda untuk memberikan pengguna Anda akses ke AWS Management Console tanpa perlu mengkonfigurasi dan mengelola infrastruktur SAML yang terpisah.

Untuk lebih meningkatkan pengalaman pengguna akhir, Anda dapat mengaktifkan kemampuan masuk tunggal untuk Amazon WorkDocs, yang memberi pengguna Anda kemampuan untuk mengakses Amazon WorkDocs dari komputer yang bergabung ke direktori tanpa harus memasukkan kredensialnya secara terpisah.

Anda dapat memberikan akses ke akun pengguna di direktori Anda atau di Direktori Aktif lokal, sehingga mereka dapat masuk ke AWS Management Console atau melalui AWS CLI menggunakan kredensyal dan izin yang ada untuk mengelola AWS sumber daya dengan menetapkan peran IAM langsung ke akun pengguna yang ada.

FSx for Windows File Server integrasi AWS dengan Microsoft AD yang Dikelola

Mengintegrasikan FSx for Windows File Server dengan Microsoft AD yang AWS Dikelola menyediakan sistem file protokol Server Message Block (SMB) berbasis Microsoft Windows asli yang dikelola sepenuhnya yang memungkinkan Anda untuk dengan mudah memindahkan aplikasi dan klien berbasis Windows Anda (yang memanfaatkan penyimpanan file bersama) ke. AWSMeskipun FSx for Windows File Server dapat diintegrasikan dengan Microsoft Active Directory yang dikelola sendiri, kami tidak membahas skenario itu di sini.

Kasus penggunaan dan sumber daya umum Amazon FSx

Bagian ini memberikan referensi ke sumber daya tentang integrasi FSx for Windows File Server umum dengan kasus penggunaan Microsoft AD yang AWS Dikelola. Setiap kasus penggunaan di bagian ini dimulai dengan konfigurasi Microsoft AD dan FSx for Windows File Server dasar yang AWS Dikelola. Untuk informasi selengkapnya tentang cara membuat konfigurasi ini, lihat:

- Memulai dengan Microsoft AD yang AWS Dikelola
- Memulai dengan Amazon FSx

FSx for Windows File Server sebagai penyimpanan persisten pada wadah Windows

Amazon Elastic Container Service (ECS) mendukung kontainer Windows pada instans kontainer yang diluncurkan dengan Windows AMI yang dioptimalkan Amazon ECS. Instans kontainer Windows menggunakan versi dari agen kontainer Amazon ECS miliknya sendiri. Pada Windows AMI yang dioptimalkan Amazon ECS, agen kontainer Amazon ECS berjalan sebagai layanan pada host.

Amazon ECS mendukung autentikasi Direktori Aktif untuk kontainer Windows melalui akun layanan khusus yang disebut group Managed Service Account (gMSA). Karena kontainer Windows tidak dapat tergabung domain, Anda harus mengonfigurasi kontainer Windows untuk berjalan dengan gMSA.

Barang Terkait

- Menggunakan fsX for Windows File Server sebagai penyimpanan persisten pada Windows Container
- Akun Layanan Terkelola Grup

Dukungan Amazon AppStream 2.0

Amazon AppStream 2.0 adalah layanan streaming aplikasi yang dikelola sepenuhnya. Ini menyediakan berbagai solusi bagi pengguna untuk menyimpan dan mengakses data melalui aplikasi mereka. Amazon FSx dengan AppStream 2.0 menyediakan drive penyimpanan persisten pribadi menggunakan Amazon FSx dan dapat dikonfigurasi untuk menyediakan folder bersama untuk mengakses file umum.

Barang Terkait

- Walkthrough 4: Menggunakan Amazon FSx dengan Amazon 2.0 AppStream

- Menggunakan Amazon FSx dengan Amazon 2.0 AppStream
- Menggunakan Active Directory dengan AppStream 2.0

Dukungan Microsoft SQL Server

FSx for Windows File Server dapat digunakan sebagai opsi penyimpanan untuk Microsoft SQL Server 2012 (dimulai dengan 2012 versi 11.x) dan database sistem yang lebih baru (termasuk Master, Model, MSDB, dan TempDB), dan untuk database pengguna Database Engine.

Barang Terkait

- Instal SQL Server dengan penyimpanan fileshare SMB
- Sederhanakan penerapan ketersediaan tinggi Microsoft SQL Server Anda menggunakan FSx for Windows File Server
- Akun Layanan Terkelola Grup

Folder rumah dan dukungan profil pengguna roaming

FSx for Windows File Server dapat digunakan untuk menyimpan data dari folder home pengguna Active Directory dan My Documents di lokasi pusat. FSx for Windows File Server juga dapat digunakan untuk menyimpan data dari Profil Pengguna Roaming.

Barang terkait

- Direktori rumah Windows menjadi mudah dengan Amazon FSx
- Menyebarkan profil pengguna roaming
- Menggunakan fsX for Windows File Server dengan WorkSpaces

Dukungan berbagi file jaringan

Berbagi file jaringan pada FSx for Windows File Server menyediakan solusi berbagi file yang dikelola dan dapat diskalakan. Satu kasus penggunaan dipetakan drive untuk klien yang dapat dibuat secara manual atau melalui Kebijakan Grup.

Barang terkait

- Walkthrough 6: Menskalakan kinerja dengan Shards
- Pemetaan drive

- Menggunakan fsX for Windows File Server dengan WorkSpaces

Dukungan instalasi perangkat lunak kebijakan grup

Karena ukuran dan performa folder SYSVOL terbatas, sebagai praktik terbaik harus, menghindari menyimpan data seperti file instalasi perangkat lunak dalam folder tersebut. Sebagai solusi yang mungkin untuk ini, FSx for Windows File Server dapat dikonfigurasi untuk menyimpan semua file perangkat lunak yang diinstal menggunakan Kebijakan Grup.

Barang terkait

- Cara menggunakan Kebijakan Grup untuk menginstal perangkat lunak dari jarak jauh di Windows Server 2008 dan di Windows Server 2003

Dukungan target Backup Server Windows

FSx for Windows File Server dapat dikonfigurasi sebagai drive target di Windows Server Backup menggunakan berbagi file UNC. Dalam hal ini, Anda akan menentukan jalur UNC ke FSx for Windows File Server Anda alih-alih ke volume EBS terlampir.

Barang Terkait

- Lakukan pemulihan status sistem server Anda

Amazon FSx juga mendukung Berbagi Direktori AWS Microsoft AD yang Dikelola. Lihat informasi yang lebih lengkap di:

- Bagikan direktori Anda
- Menggunakan Amazon FSx dengan AWS Microsoft AD yang Dikelola di VPC atau akun yang berbeda

Integrasi Amazon RDS dengan Microsoft AD yang AWS Dikelola

Amazon RDS mendukung autentikasi eksternal pengguna basis data menggunakan Kerberos dan Microsoft Active Directory. Kerberos adalah protokol autentikasi jaringan yang menggunakan tiket dan kriptografi kunci-simetris untuk menghilangkan kebutuhan untuk mentransmisikan kata sandi melalui jaringan. Dukungan Amazon RDS untuk Kerberos dan Direktori Aktif menyediakan

keuntungan dari sign-on tunggal dan autentikasi terpusat dari pengguna basis data sehingga Anda dapat menyimpan kredensial pengguna Anda di Direktori Aktif.

Untuk memulai kasus penggunaan ini, pertama-tama Anda harus menyiapkan konfigurasi Microsoft AD dan Amazon RDS yang AWS Dikelola dasar.

- Memulai dengan Microsoft AD yang AWS Dikelola
- Memulai dengan Amazon RDS

Semua kasus penggunaan yang dirujuk di bawah ini akan dimulai dengan basis Microsoft AD dan Amazon RDS yang AWS dikelola dan mencakup cara mengintegrasikan Amazon RDS dengan AWS Microsoft AD yang Dikelola.

- Menggunakan otentikasi Windows dengan instans Amazon RDS for SQL Server DB
- Menggunakan otentikasi Kerberos untuk MySQL
- Menggunakan otentikasi Kerberos dengan Amazon RDS for Oracle
- Menggunakan otentikasi Kerberos dengan Amazon RDS for PostgreSQL

Amazon RDS juga mendukung Berbagi Direktori Microsoft AD yang AWS Dikelola. Lihat informasi yang lebih lengkap di:

- Bagikan direktori Anda
- Bergabung dengan instans Amazon RDS DB Anda di seluruh akun ke satu domain bersama

Untuk informasi selengkapnya tentang menggabungkan Amazon RDS for SQL Server ke Active Directory, lihat Bergabung dengan Amazon RDS for SQL Server ke Active Directory yang dikelola sendiri.

Aplikasi .NET menggunakan Amazon RDS for SQL Server dengan Akun Layanan Terkelola grup

Anda dapat mengintegrasikan Amazon RDS for SQL Server dengan aplikasi .NET dasar dan Akun Layanan Terkelola grup (gMSAs). Untuk informasi selengkapnya, lihat Cara Microsoft AD yang AWS Dikelola Membantu Menyederhanakan Penerapan dan Meningkatkan Keamanan Direktori Aktif—Aplikasi .NET Terintegrasi

Kasus Penggunaan 2: Mengelola instans Amazon EC2

Dengan menggunakan alat administrasi Direktori Aktif yang sudah dikenal, Anda dapat menerapkan objek kebijakan grup Active Directory (GPO) untuk mengelola instans Amazon EC2 untuk Windows atau Linux secara terpusat dengan menggabungkan instans ke domain Microsoft AD yang AWS Dikelola.

Selain itu, pengguna Anda dapat masuk ke instans Anda dengan kredensyal Direktori Aktif mereka. Ini menghilangkan kebutuhan untuk menggunakan kredensial instans individu atau mendistribusikan file kunci pribadi (PEM). Ini memudahkan Anda untuk langsung memberikan atau mencabut akses ke pengguna dengan menggunakan alat administrasi pengguna Active Directory yang sudah Anda gunakan.

Kasus Penggunaan 3: Menyediakan layanan direktori ke beban kerja yang sadar Direktori Aktif

AWS Microsoft AD yang dikelola adalah Microsoft Active Directory aktual yang memungkinkan Anda menjalankan beban kerja tradisional yang sadar Active Directory seperti Remote Desktop Licensing Manager dan Microsoft SharePoint dan Microsoft SQL Server Always On di Cloud. AWS AWS Microsoft AD yang dikelola juga membantu Anda menyederhanakan dan meningkatkan keamanan aplikasi.NET yang terintegrasi dengan Direktori Aktif dengan menggunakan Akun Layanan Terkelola grup (GMSAs) dan delegasi terbatas Kerberos (KCD).

Kasus Penggunaan 4: AWS IAM Identity Center ke Office 365 dan aplikasi cloud lainnya

Anda dapat menggunakan Microsoft AD yang AWS Dikelola AWS IAM Identity Center untuk menyediakan aplikasi cloud. Anda dapat menggunakan Microsoft Entra Connect (sebelumnya dikenal sebagaiAzure Active Directory Connect) untuk menyinkronkan pengguna Anda ke Microsoft Entra (sebelumnya dikenal sebagai Azure Active Directory (AzureAD)), dan kemudian menggunakan Active Directory Federation Services (AD FS) sehingga pengguna Anda dapat mengakses Microsoft Office 365 dan aplikasi cloud SAMP 2.0 lainnya dengan menggunakan kredensyal Active Directory mereka.

Mengintegrasikan Microsoft AD AWS Terkelola dengan IAM Identity Center menambahkan kemampuan SAMP ke AWS Microsoft AD dan/yang Dikelola atau domain tepercaya lokal Anda. Setelah terintegrasi, pengguna Anda dapat menggunakan IAM Identity Center dengan layanan yang mendukung SAMP, termasuk aplikasi cloud pihak ketiga AWS Management Console dan pihak ketiga seperti Office 365, Concur, dan Salesforce tanpa harus mengonfigurasi infrastruktur SAMP.

Untuk demonstrasi tentang proses mengizinkan pengguna lokal menggunakan Pusat Identitas IAM, lihat video berikut. YouTube

> **Note**
>
> AWS Single Sign-On diubah namanya menjadi IAM Identity Center.

Kasus Penggunaan 5: Memperluas Direktori Aktif lokal Anda ke Cloud AWS

Jika Anda sudah memiliki infrastruktur Direktori Aktif dan ingin menggunakannya saat memigrasikan beban kerja Active Directory-aware ke Cloud AWS , AWS Microsoft AD yang Dikelola dapat membantu. Anda dapat menggunakan trust Active Directory untuk menghubungkan AD Microsoft AWS Terkelola ke Active Directory yang ada. Ini berarti pengguna Anda dapat mengakses Active Directory-aware dan AWS aplikasi dengan kredensyal Active Directory lokal mereka, tanpa perlu Anda menyinkronkan pengguna, grup, atau kata sandi.

Misalnya, pengguna Anda dapat masuk ke Amazon AWS Management Console dan Amazon WorkSpaces dengan menggunakan nama pengguna dan kata sandi Active Directory yang ada. Selain itu, saat Anda menggunakan aplikasi Active Directory-aware seperti dengan AWS Microsoft AD yang SharePoint Dikelola, pengguna Windows yang masuk dapat mengakses aplikasi ini tanpa perlu memasukkan kredensyal lagi.

Anda juga dapat memigrasikan domain Active Directory lokal AWS agar bebas dari beban operasional infrastruktur Active Directory menggunakan Active Directory Migration Toolkit (ADMT) bersama dengan Layanan Ekspor Kata Sandi (PES) untuk melakukan migrasi.

Kasus Penggunaan 6: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh akun AWS

Berbagi direktori Anda di beberapa AWS akun memungkinkan Anda mengelola AWS layanan seperti Amazon EC2 dengan mudah tanpa perlu mengoperasikan direktori untuk setiap akun dan setiap VPC. Anda dapat menggunakan direktori Anda dari akun AWS mana pun dan dari Amazon VPC mana pun dalam Region AWS . Kemampuan ini membuatnya lebih mudah dan lebih hemat biaya untuk mengelola beban kerja sadar direktori dengan satu direktori di seluruh akun dan VPC. Misalnya, Anda sekarang dapat mengelola Beban kerja Windows Anda yang di-deploy di instans EC2 di beberapa akun dan VPC dengan mudah menggunakan direktori Microsoft AD yang Dikelola AWS .

Saat membagikan direktori Microsoft AD AWS Terkelola dengan AWS akun lain, Anda dapat menggunakan konsol Amazon EC2 atau AWS Systems Managerbergabung dengan instans Anda dengan mulus dari VPC Amazon apa pun dalam akun dan Wilayah. AWS Anda dapat dengan cepat men-deploy beban kerja sadar direktori pada instans EC2 dengan menghilangkan kebutuhan untuk secara manual menggabungkan instans Anda ke domain atau untuk men-deploy direktori di setiap akun dan VPC. Untuk informasi selengkapnya, lihat Bagikan direktori Anda.

Cara mengelola Microsoft AD yang Dikelola AWS

Bagian ini berisi daftar semua prosedur untuk mengoperasikan dan memelihara lingkungan Microsoft AD yang Dikelola AWS.

Topik

Mengamankan direktori Microsoft AD yang Dikelola AWS Anda

Bagian ini menjelaskan pertimbangan untuk mengamankan lingkungan Microsoft AD yang Dikelola AWS.

Topik

- Mengelola kebijakan kata sandi untuk Microsoft AD yang AWS Dikelola
- Mengaktifkan autentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS
- Aktifkan LDAP atau LDAPS yang aman
- Mengelola kepatuhan untuk Microsoft AD yang Dikelola AWS
- Meningkatkan konfigurasi keamanan jaringan Microsoft AD yang Dikelola AWS Anda
- Konfigurasikan pengaturan keamanan direktori
- Siapkan AWS Private CA Konektor untuk AD

Mengelola kebijakan kata sandi untuk Microsoft AD yang AWS Dikelola

AWS Microsoft AD yang dikelola memungkinkan Anda menentukan dan menetapkan kebijakan penguncian kata sandi dan akun yang berbeda (juga disebut sebagai kebijakan kata sandi berbutir halus) untuk grup pengguna yang Anda kelola di domain Microsoft AD Terkelola AWS . Saat Anda membuat direktori Microsoft AD AWS Terkelola, kebijakan domain default dibuat dan diterapkan ke direktori tersebutActive Directory. Kebijakan ini mencakup pengaturan berikut:

Kebijakan	Pengaturan
Memberlakukan riwayat kata sandi	24 kata sandi diingat
Usia kata sandi maksimal	42 hari *
Usia kata sandi minimum	1 hari
Panjang kata sandi minimum	7 karakter
Kata sandi harus memenuhi persyaratan kompleksitas	Diaktifkan
Menyimpan kata sandi menggunakan enkripsi reversibel	Nonaktif

* Catatan: Usia maksimum sandi 42 hari termasuk kata sandi admin.

Misalnya, Anda dapat menetapkan pengaturan kebijakan yang kurang ketat untuk karyawan yang memiliki akses ke informasi sensitivitas rendah saja. Untuk manajer senior yang secara teratur mengakses informasi rahasia Anda dapat menerapkan pengaturan yang lebih ketat.

Berikut ini adalah sumber daya untuk mempelajari lebih lanjut tentang kebijakan kata sandi dan kebijakan Microsoft Active Directory keamanan berbutir halus:

- Konfigurasikan setelan kebijakan keamanan
- Persyaratan kompleksitas kata sandi
- Pertimbangan keamanan kompleksitas kata sandi

AWS menyediakan serangkaian kebijakan kata sandi berbutir halus di AWS Microsoft AD Terkelola yang dapat Anda konfigurasikan dan tetapkan ke grup Anda. Untuk mengonfigurasi kebijakan, Anda dapat menggunakan alat Microsoft kebijakan standar seperti Pusat Active Directory Administratif. Untuk memulai dengan alat Microsoft kebijakan, lihatInstal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola.

Bagaimana kebijakan kata sandi diterapkan

Ada perbedaan dalam bagaimana kebijakan kata sandi berbutir halus diterapkan tergantung pada apakah kata sandi disetel ulang atau kata sandi diubah. Pengguna domain dapat mengubah kata sandi mereka sendiri. Active DirectoryAdministrator atau pengguna dengan izin yang diperlukan dapat mengatur ulang kata sandi pengguna. Lihat bagan berikut untuk informasi lebih lanjut.

Kebijakan	Reset Kata Sandi	Perubahan Kata Sandi
Memberlakukan riwayat kata sandi	Tida	Ya
Usia kata sandi maksimal	Ya	Ya
Usia kata sandi minimum	Tida	Ya
Panjang kata sandi minimum	Ya	Ya

Kebijakan	Reset Kata Sandi	Perubahan Kata Sandi
Kata sandi harus memenuhi persyaratan kompleksitas	 Ya	 Ya

Perbedaan ini memiliki implikasi keamanan. Misalnya, setiap kali kata sandi pengguna disetel ulang, riwayat penegakan kata sandi dan kebijakan usia kata sandi minimum tidak diberlakukan. Untuk informasi selengkapnya, lihat dokumentasi Microsoft tentang pertimbangan keamanan yang terkait dengan menerapkan riwayat kata sandi dan kebijakan usia kata sandi minimum.

Topik

- Pengaturan kebijakan yang didukung
- Mendelegasikan siapa yang dapat mengelola kebijakan kata sandi Anda
- Menetapkan kebijakan kata sandi ke pengguna Anda

Artikel blog AWS Keamanan Terkait

- Cara mengonfigurasi kebijakan kata sandi yang lebih kuat untuk membantu memenuhi standar keamanan Anda dengan menggunakan AWS Directory Service untuk Microsoft AD yang AWS Dikelola

Pengaturan kebijakan yang didukung

AWS Microsoft AD yang dikelola mencakup lima kebijakan berbutir halus dengan nilai prioritas yang tidak dapat diedit. Kebijakan memiliki sejumlah properti yang dapat Anda konfigurasikan untuk memberlakukan kekuatan kata sandi, dan tindakan penguncian akun jika terjadi peristiwa kegagalan login. Anda dapat menetapkan kebijakan ke nol atau lebih grup Direktori Aktif. Jika pengguna akhir adalah anggota dari beberapa grup dan menerima lebih dari satu kebijakan kata sandi, Direktori Aktif memberlakukan kebijakan dengan nilai prioritas terendah.

AWS kebijakan kata sandi yang telah ditentukan sebelumnya

Tabel berikut mencantumkan lima kebijakan yang disertakan dalam direktori AD Microsoft AWS Terkelola dan nilai prioritas yang ditetapkan. Untuk informasi selengkapnya, lihat Precedence.

Nama kebijakan	Precedence
PelangganPSO-01	10
PelangganPSO-02	20
PelangganPSO-03	30
PelangganPSO-04	40
PelangganPSO-05	50

Properti kebijakan kata sandi

Anda dapat mengedit properti berikut dalam kebijakan kata sandi agar sesuai dengan standar kepatuhan yang memenuhi kebutuhan bisnis Anda.

- Nama kebijakan
- Menegakkan riwayat kata sandi
- Panjang kata sandi minimum
- Usia kata sandi minimum
- Usia kata sandi maksimum
- Simpan kata sandi menggunakan enkripsi reversibel
- Kata sandi harus memenuhi persyaratan kompleksitas

Anda tidak dapat mengubah nilai prioritas untuk kebijakan ini. Untuk detail selengkapnya tentang bagaimana pengaturan ini memengaruhi penegakan kata sandi, lihat AD DS: Kebijakan kata sandi berbutir halus di situs web Microsoft. TechNet Untuk informasi umum tentang kebijakan ini, lihat Kebijakan kata sandi di TechNet situs web Microsoft.

Kebijakan penguncian akun

Anda juga dapat mengubah properti berikut dari kebijakan kata sandi Anda untuk menentukan apakah dan bagaimana Direktori Aktif harus mengunci akun setelah kegagalan login:

- Jumlah upaya masuk yang gagal diizinkan
- Durasi penguncian akun

- Mengatur ulang upaya masuk yang gagal setelah beberapa durasi

Untuk informasi umum tentang kebijakan ini, lihat Kebijakan penguncian akun di TechNet situs web Microsoft.

Precedence

Kebijakan dengan nilai prioritas yang lebih rendah memiliki prioritas yang lebih tinggi. Anda menetapkan kebijakan kata sandi untuk grup keamanan Direktori Aktif. Meskipun Anda harus menerapkan kebijakan tunggal untuk grup keamanan, satu pengguna tunggal mungkin menerima lebih dari satu kebijakan kata sandi. Sebagai contoh, misalkan `jsmith` adalah anggota dari grup HR dan juga anggota dari grup MANAJER. Jika Anda menetapkan CustomerPSO-05 (yang memiliki prioritas 50) untuk grup HR, dan CustomerPSO-04 (yang memiliki prioritas 40) untuk MANAJER, CustomerPSO-04 memiliki prioritas yang lebih tinggi dan Direktori Aktif menerapkan kebijakan tersebut untuk `jsmith`.

Jika Anda menetapkan beberapa kebijakan untuk pengguna atau grup, Direktori Aktif menentukan kebijakan yang dihasilkan sebagai berikut:

1. Kebijakan yang Anda tetapkan langsung ke objek pengguna berlaku.
2. Jika tidak ada kebijakan yang diberikan langsung ke objek pengguna, kebijakan dengan nilai prioritas terendah dari semua kebijakan yang diterima oleh pengguna sebagai hasil dari keanggotaan grup berlaku.

Untuk detail tambahan, lihat AD DS: Kebijakan kata sandi berbutir halus di situs web Microsoft. TechNet

Mendelegasikan siapa yang dapat mengelola kebijakan kata sandi Anda

Anda dapat mendelegasikan izin untuk mengelola kebijakan kata sandi ke akun pengguna tertentu yang Anda buat di AWS Microsoft AD Terkelola dengan menambahkan akun ke grup keamanan Administrator Kebijakan Kata Sandi Berbutir Halus yang AWS Delegasi. Ketika sebuah akun menjadi anggota grup ini, akun tersebut memiliki izin untuk mengedit dan mengkonfigurasi salah satu kebijakan kata sandi yang tercantum sebelumnya.

Untuk mendelegasikan siapa yang dapat mengelola kebijakan kata sandi

1. Luncurkan Pusat Administratif Direktori Aktif (ADAC) dari instans EC2 terkelola yang Anda gabungkan ke domain AWS Microsoft AD Terkelola.

2. Beralih ke Tampilan pohon dan arahkan ke OU AWS Grup yang didelegasikan. Untuk informasi selengkapnya tentang OU ini, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.
3. Temukan pengguna grup Administrator Kebijakan Kata Sandi Terperinci yang Didelegasikan AWS . Menambahkan setiap pengguna atau grup dari domain Anda ke grup ini.

Menetapkan kebijakan kata sandi ke pengguna Anda

Akun pengguna yang merupakan anggota grup keamanan Administrator Kebijakan Kata Sandi Terperinci yang Didelegasikan AWS dapat menggunakan prosedur berikut untuk menetapkan kebijakan untuk pengguna dan grup keamanan.

Untuk menetapkan kebijakan kata sandi ke pengguna Anda

1. Luncurkan Pusat Administratif Direktori Aktif (ADAC) dari instans EC2 terkelola yang Anda gabungkan ke domain AWS Microsoft AD Terkelola.
2. Beralih ke Tampilan pohon dan arahkan ke Kontainer pengaturan Sistem\Kata sandi.
3. Klik dua kali pada kebijakan terperinci yang ingin Anda edit. Klik Tambahkan untuk mengedit properti kebijakan, dan menambahkan pengguna atau grup keamanan ke kebijakan tersebut. Untuk informasi selengkapnya tentang kebijakan terperinci default yang disediakan dengan Microsoft AD yang Dikelola AWS , lihat AWS kebijakan kata sandi yang telah ditentukan sebelumnya.
4. Untuk memverifikasi kebijakan kata sandi telah diterapkan, jalankan PowerShell perintah berikut:

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

> **Note**
>
> Hindari menggunakan `net user` perintah karena hasilnya bisa tidak akurat.

Jika Anda tidak mengonfigurasi salah satu dari lima kebijakan kata sandi di direktori Microsoft AD AWS Terkelola, Active Directory menggunakan kebijakan grup domain default. Untuk detail tambahan tentang penggunaan Kontainer pengaturan kata sandi, lihat Postingan blog Microsoft.

Mengaktifkan autentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS

Anda dapat mengaktifkan multi-factor authentication (MFA) untuk direktori Microsoft AD yang Dikelola AWS untuk meningkatkan keamanan ketika pengguna Anda menentukan kredensial AD-nya untuk mengakses Aplikasi Amazon Enterprise yang didukung. Saat Anda mengaktifkan MFA, pengguna Anda memasukkan nama pengguna dan kata sandi mereka (faktor pertama) seperti biasa, dan mereka juga harus memasukkan kode autentikasi (faktor kedua) yang mereka dapatkan dari solusi MFA virtual atau perangkat keras Anda. Faktor-faktor ini bersama-sama memberikan keamanan tambahan dengan mencegah akses ke aplikasi Amazon Enterprise Anda, kecuali pengguna menyediakan kredensial pengguna yang valid dan kode MFA yang valid.

Untuk mengaktifkan MFA, Anda harus memiliki solusi MFA yang adalah server Layanan autentikasi jarak jauh panggilan masuk pengguna (RADIUS), atau Anda harus memiliki plugin MFA ke server RADIUS yang sudah diterapkan di infrastruktur on-premise Anda. Solusi MFA Anda harus menerapkan Kode Sandi Sekali Pakai (OTP) yang diperoleh pengguna dari perangkat keras atau dari perangkat lunak yang berjalan pada perangkat seperti ponsel.

RADIUS adalah standar industri client/server protokol yang menyediakan autentikasi, otorisasi, dan manajemen akuntansi untuk memungkinkan pengguna untuk terhubung ke layanan jaringan. AWS Microsoft AD terkelola termasuk klien RADIUS yang menghubungkan ke server RADIUS di mana Anda telah menerapkan solusi MFA Anda. Server RADIUS Anda memvalidasi nama pengguna dan kode OTP. Jika server RADIUS Anda berhasil memvalidasi pengguna, Microsoft AD yang AWS dikelola kemudian mengautentikasi pengguna terhadap Active Directory. Setelah otentikasi Active Directory berhasil, pengguna kemudian dapat mengakses AWS aplikasi. Komunikasi antara klien RADIUS Microsoft AD yang Dikelola AWS dan server RADIUS Anda memerlukan Anda untuk mengkonfigurasi grup keamanan AWS yang memungkinkan komunikasi melalui port 1812.

Anda dapat mengaktifkan autentikasi multi-faktor untuk direktori Microsoft AD yang Dikelola AWS dengan melakukan prosedur berikut. Untuk informasi selengkapnya tentang cara mengkonfigurasi server RADIUS Anda untuk bekerja dengan AWS Directory Service dan MFA, lihat Prasyarat autentikasi multi-faktor.

> **Note**
>
> Autentikasi multi-faktor tidak tersedia untuk Simple AD. Namun, MFA dapat diaktifkan untuk direktori AD Connector Anda. Untuk informasi selengkapnya, lihat Mengaktifkan autentikasi multi-faktor untuk AD Connector.

> **Note**
>
> MFA adalah fitur Regional dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk mengaktifkan autentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS

1. Identifikasi alamat IP server autentikasi multi-faktor (MFA) RADIUS Anda dan direktori Microsoft AD yang Dikelola AWS Anda.
2. Edit grup keamanan Virtual Private Cloud (VPC) Anda untuk mengaktifkan komunikasi melalui port 1812 antara titik akhir IP Microsoft AD yang Dikelola AWS dan server autentikasi multi-faktor (MFA) RADIUS Anda.
3. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
4. Pilih tautan ID direktori untuk direktori Microsoft AD yang Dikelola AWS Anda.
5. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan autentikasi multi-faktor (MFA), lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
6. Di bagian Autentikasi multi-faktor, pilih Tindakan, lalu pilih Aktifkan.
7. Pada halaman Aktifkan multi-factor authentication (MFA), berikan nilai berikut:

   Label tampilan

   Berikan nama label.

   Nama DNS server RADIUS atau alamat IP

   Alamat IP titik akhir server RADIUS, atau alamat IP penyeimbang beban server RADIUS. Anda dapat memasukkan beberapa alamat IP dengan memisahkannya dengan koma (misalnya, `192.0.0.0,192.0.0.12`).

> **Note**
>
> RADIUS MFA hanya berlaku untuk mengautentikasi akses keAWS Management Console, atau ke aplikasi dan layanan Amazon Enterprise seperti, WorkSpaces Amazon, atau Amazon QuickSight Chime. Ini tidak menyediakan autentikasi multi-faktor (MFA) ke beban kerja Windows yang berjalan pada instans EC2, atau untuk masuk ke instans EC2. AWS Directory Service tidak mendukung autentikasi Tantangan/Tanggapan RADIUS.
> Pengguna harus memiliki kode autentikasi multi-faktor (MFA) mereka pada saat mereka memasukkan nama pengguna dan kata sandi. Atau, Anda harus menggunakan solusi yang melakukan MFA out-of-band seperti verifikasi teks SMS untuk pengguna. Dalam solusi out-of-band MFA, Anda harus memastikan bahwa Anda menetapkan nilai batas waktu RADIUS dengan tepat untuk solusi Anda. Saat menggunakan solusi out-of-band MFA, halaman masuk akan meminta pengguna untuk kode MFA. Dalam hal ini, pengguna harus memasukkan kata sandi mereka di bidang kata sandi dan bidang MFA.

Pelabuhan

Port yang digunakan oleh server RADIUS Anda untuk komunikasi. Jaringan on-premise Anda harus mengizinkan lalu lintas masuk melalui port server RADIUS default (UDP:1812) dari server AWS Directory Service.

Kode rahasia bersama

Kode rahasia bersama yang ditentukan ketika titik akhir RADIUS Anda dibuat.

Konfirmasikan kode rahasia bersama

Konfirmasi kode rahasia bersama untuk titik akhir RADIUS Anda.

Protokol

Pilih protokol yang ditentukan saat titik akhir RADIUS Anda dibuat.

Batas waktu server (dalam hitungan detik)

Jumlah waktu, dalam detik, untuk menunggu server RADIUS menanggapi. Ini harus berupa nilai antara 1 dan 50.

> **Note**
>
> Sebaiknya konfigurasi batas waktu server RADIUS Anda menjadi 20 detik atau kurang. Jika batas waktu melebihi 20 detik, sistem tidak dapat mencoba lagi dengan server RADIUS lain dan dapat mengakibatkan kegagalan batas waktu.

Permintaan Max RADIUS mencoba ulang

Berapa kali komunikasi dengan server RADIUS dicoba. Ini harus berupa nilai antara 0 dan 10.

Autentikasi multi-faktor tersedia ketika Status RADIUS berubah ke Diaktifkan.

8. Pilih Aktifkan.

Aplikasi Amazon Enterprise yang didukung

Semua aplikasi TI Amazon Enterprise termasuk WorkSpaces, Amazon WorkDocs, Amazon WorkMail, Amazon QuickSight, dan akses ke AWS IAM Identity Center dan AWS Management Console didukung saat menggunakan Konektor AD dan AD Microsoft AWS Terkelola dengan MFA.

Untuk informasi tentang cara mengkonfigurasi akses pengguna dasar ke aplikasi Amazon Enterprise, Sign-On Tunggal AWS dan AWS Management Consolemenggunakan AWS Directory Service, lihat Aktifkan akses ke AWS aplikasi dan layanan dan Mengaktifkan akses ke AWS Management Console dengan kredensial AD.

Artikel blog AWS Keamanan Terkait

- Cara mengaktifkan autentikasi multi-faktor untuk AWS layanan dengan menggunakan Managed AWS Microsoft AD dan kredensi lokal

Aktifkan LDAP atau LDAPS yang aman

Lightweight Directory Access Protocol (LDAP) adalah protokol komunikasi standar yang digunakan untuk membaca dan menulis data ke dan dari Direktori Aktif. Beberapa aplikasi menggunakan LDAP untuk menambah, menghapus, atau mencari pengguna dan grup di Direktori Aktif atau untuk

mengangkut kredensial untuk autentikasi pengguna di Direktori Aktif. Setiap komunikasi LDAP termasuk klien (seperti aplikasi) dan server (seperti Direktori Aktif).

Secara default, komunikasi melalui LDAP tidak dienkripsi. Hal ini memungkinkan bagi pengguna berbahaya untuk menggunakan perangkat lunak pemantauan jaringan untuk melihat paket data melalui kabel. Inilah sebabnya mengapa banyak kebijakan keamanan perusahaan biasanya mengharuskan organisasi mengenkripsi semua komunikasi LDAP.

Untuk mengurangi bentuk paparan data ini, AWS Microsoft AD yang dikelola menyediakan opsi: Anda dapat mengaktifkan LDAP melalui Secure Sockets Layer (SSL) /Transport Layer Security (TLS), juga dikenal sebagai LDAPS. Dengan LDAPS, Anda dapat meningkatkan keamanan di seluruh kabel. Anda juga dapat memenuhi persyaratan kepatuhan dengan mengenkripsi semua komunikasi antara aplikasi berkemampuan LDAP dan Microsoft AD yang Dikelola. AWS

AWS Microsoft AD yang dikelola menyediakan dukungan untuk LDAPS dalam skenario penerapan berikut:

- LDAPS sisi server mengenkripsi komunikasi LDAP antara aplikasi sadar LDAP komersial atau lokal Anda (bertindak sebagai klien LDAP) dan Microsoft AD Terkelola (bertindak sebagai server LDAP). AWS Untuk informasi selengkapnya, lihat Aktifkan LDAPS sisi server menggunakan Microsoft AD yang Dikelola AWS.
- LDAPS sisi klien mengenkripsi komunikasi LDAP antara AWS aplikasi seperti WorkSpaces (bertindak sebagai klien LDAP) dan Direktori Aktif yang dikelola sendiri (lokal) Anda (bertindak sebagai server LDAP). Untuk informasi selengkapnya, lihat Aktifkan LDAPS sisi klien menggunakan Microsoft AD yang Dikelola AWS.

Topik

Aktifkan LDAPS sisi server menggunakan Microsoft AD yang Dikelola AWS

Protokol Akses Direktori Ringan sisi Server Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) mendukung mengenkripsi komunikasi LDAP antara aplikasi sadar LDAP komersial atau lokal dan direktori Microsoft AD Anda yang Dikelola. AWS Ini membantu untuk meningkatkan keamanan di seluruh kabel dan memenuhi persyaratan kepatuhan menggunakan protokol kriptografi Lapisan Soket Aman (SSL).

Aktifkan LDAPS sisi server

Untuk petunjuk terperinci tentang cara mengatur dan mengonfigurasi LDAPS sisi server dan server otoritas sertifikat (CA) Anda, lihat Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD Terkelola Anda AWS di Blog Keamanan. AWS

Anda harus melakukan sebagian besar pengaturan dari instans Amazon EC2 yang Anda gunakan untuk mengelola pengendali domain Microsoft AD yang Dikelola AWS Anda. Langkah-langkah berikut memandu Anda untuk mengaktifkan LDAPS untuk domain Anda di Cloud. AWS

Jika Anda ingin menggunakan otomatisasi untuk mengatur Infrastruktur PKI Anda, Anda dapat menggunakan Infrastruktur Kunci Publik Microsoft pada AWS QuickStart Panduan. Secara khusus Anda akan ingin mengikuti petunjuk dalam panduan untuk memuat templat untuk Men-deploy Microsoft PKI ke VPC yang sudah ada pada AWS. Setelah Anda memuat templat, pastikan untuk memilih **`AWSManaged`** saat Anda sampai ke opsi Jenis Layanan Domain Direktori Aktif. Jika Anda menggunakan QuickStart panduan ini, Anda dapat melompat langsung keLangkah 3: Membuat templat sertifikat.

Topik

- Langkah 1: Delegasikan yang dapat mengaktifkan LDAPS
- Langkah 2: Mengatur otoritas sertifikat Anda
- Langkah 3: Membuat templat sertifikat
- Langkah 4: Menambahkan aturan grup keamanan

Langkah 1: Delegasikan yang dapat mengaktifkan LDAPS

Untuk mengaktifkan LDAPS sisi server, Anda harus menjadi anggota grup Admin atau Administrator Otoritas Sertifikat Perusahaan yang AWS Delegasi di direktori Microsoft AD yang Dikelola. AWS Atau, Anda dapat menjadi pengguna administratif default (akun Admin). Jika mau, Anda dapat memiliki pengguna selain LDAPS pengaturan akun Admin. Jika demikian, tambahkan pengguna tersebut ke grup Admin atau Administrator Otoritas Sertifikat Perusahaan AWS yang Delegasi di direktori AD AWS Microsoft Terkelola Anda.

Langkah 2: Mengatur otoritas sertifikat Anda

Sebelum Anda dapat mengaktifkan LDAPS sisi server, Anda harus membuat sertifikat. Sertifikat ini harus dikeluarkan oleh server Microsoft Enterprise CA yang bergabung dengan domain Microsoft AD

AWS Terkelola Anda. Setelah dibuat, sertifikat harus diinstal pada masing-masing pengendali domain Anda di domain tersebut. Sertifikat ini memungkinkan layanan LDAP pada pengendali domain mendengarkan dan secara otomatis menerima koneksi SSL dari klien LDAP.

> **Note**
>
> LDAPS sisi server dengan Microsoft AD yang AWS Dikelola tidak mendukung sertifikat yang dikeluarkan oleh CA mandiri. Itu juga tidak mendukung sertifikat yang dikeluarkan oleh otoritas sertifikasi pihak ketiga.

Tergantung pada kebutuhan bisnis Anda, Anda memiliki pilihan berikut untuk mengatur atau menghubungkan ke CA di domain Anda:

- Buat bawahan Microsoft Enterprise CA — (Disarankan) Dengan opsi ini, Anda dapat menggunakan server CA perusahaan Microsoft bawahan di AWS Cloud. Server tersebut dapat menggunakan Amazon EC2 sehingga bekerja dengan root Microsoft CA yang ada. Untuk informasi selengkapnya tentang cara menyiapkan CA perusahaan Microsoft bawahan, lihat Langkah 4: Menambahkan Microsoft Enterprise CA ke direktori AWS Microsoft AD Anda di Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD yang Dikelola. AWS
- Buat root Microsoft enterprise CA — Dengan opsi ini, Anda dapat membuat root Microsoft enterprise CA di AWS Cloud menggunakan Amazon EC2 dan menggabungkannya ke domain AWS Microsoft AD yang Dikelola. Root CA ini dapat mengeluarkan sertifikat untuk pengendali domain Anda. Untuk informasi selengkapnya tentang menyiapkan CA root baru, lihat Langkah 3: Menginstal dan mengonfigurasi CA offline di Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD yang Dikelola AWS Anda.

Untuk informasi selengkapnya tentang cara menggabungkan instans EC2 Anda ke domain, lihat Bergabunglah dengan instans Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola.

Langkah 3: Membuat templat sertifikat

Setelah CA korporasi Anda telah diatur, Anda dapat mengkonfigurasi templat sertifikat autentikasi Kerberos.

Membuat templat sertifikat

1. Luncurkan Pengelola Server Microsoft Windows Pilih Alat > Otoritas Sertifikasi.

2. Di jendela Otoritas Sertifikat, perluas pohon Otoritas Sertifikat di panel kiri. Klik kanan Templat Sertifikat, dan pilih Kelola.
3. Di jendela Konsol Templat Sertifikat, klik kanan Autentikasi Kerberos dan pilih Templat Duplikasi.
4. Jendela Properti Templat Baru akan muncul.
5. Di jendela Properti Templat Baru, pergi ke tab Kompatibilitas, dan kemudian lakukan hal berikut:

   a. Ubah Otoritas Sertifikasi ke OS yang cocok dengan CA Anda.

   b. Jika jendela Perubahan yang dihasilkan muncul, pilih OK.

   c. Ubah penerima Sertifikasi ke Windows 10/Windows Server 2019.

   > **Note**
   >
   > AWS Microsoft AD yang dikelola didukung oleh Windows Server 2019.

   d. Jika jendela Perubahan yang dihasilkan muncul, pilih OK.
6. Klik tab Umum dan ubah Nama tampilan templat ke LDAPOverSSL atau nama lain yang Anda inginkan.
7. Klik tab Keamanan, dan pilih Pengontrol domain di bagian Nama grup atau pengguna. Di bagian Izin untuk Pengendali Domain, verifikasi bahwa kotak centang Izinkan untuk Baca, Mendaftar, danAutoenroll dicentang.
8. Pilih OK untuk membuat templat sertifikat LDAPOverSSL (atau nama yang Anda tentukan di atas). Tutup jendela Konsol Templat Sertifikat.
9. Di jendela Otoritas Sertifikat, klik kanan Templat Sertifikat, dan pilih Baru > Templat Sertifikat untuk Diterbitkan.
10. Di jendela Aktifkan Template Sertifikat, pilih LDAPOverSSL (atau nama yang Anda tentukan di atas), lalu pilih OK.

Langkah 4: Menambahkan aturan grup keamanan

Pada langkah terakhir, Anda harus membuka konsol Amazon EC2 dan menambahkan aturan grup keamanan. Aturan-aturan ini mengizinkan pengontrol domain Anda untuk terhubung ke CA korporasi Anda untuk meminta sertifikat. Untuk melakukannya, Anda menambahkan aturan masuk sehingga CA korporasi Anda dapat menerima lalu lintas masuk dari pengendali domain Anda. Kemudian Anda menambahkan aturan keluar untuk mengizinkan lalu lintas dari pengendali domain Anda untuk CA korporasi.

Setelah kedua aturan telah dikonfigurasi, pengendali domain Anda meminta sertifikat dari CA korporasi Anda secara otomatis dan mengaktifkan LDAPS untuk direktori Anda. Layanan LDAP pada pengendali domain Anda sekarang siap untuk menerima koneksi LDAPS.

Mengonfigurasi aturan grup keamanan

1. Arahkan ke konsol Amazon EC2 Anda di https://console.aws.amazon.com/ec2 dan masuk dengan kredensial administrator.
2. Di panel kiri, pilih Kelompok Keamanan di bawah Jaringan & Keamanan.
3. Di panel utama, pilih grup AWS keamanan untuk CA Anda.
4. Pilih tab Masuk, lalu pilih Edit .
5. Di kotak dialog Edit aturan masuk, lakukan hal berikut:
   - Pilih Tambahkan aturan.
   - Pilih Semua Lalu lintas untuk Jenis dan Khususuntuk Sumber.
   - Masukkan grup AWS keamanan direktori Anda (misalnya, sg-123456789) di kotak di sebelah Sumber.
   - Pilih Simpan.
6. Sekarang pilih grup AWS keamanan direktori Microsoft AD AWS Terkelola Anda. Pilih tab Keluar, lalu pilih Edit.
7. Di kotak dialog Edit aturan keluar, lakukan hal berikut:
   - Pilih Tambahkan aturan.
   - Pilih Semua Lalu lintas untuk Jenis dan Khususuntuk Tujuan.
   - Ketik grup AWS keamanan CA Anda di kotak di sebelah Tujuan.
   - Pilih Simpan.

Anda dapat menguji koneksi LDAPS ke direktori AWS Microsoft AD yang Dikelola menggunakan alat LDP. Alat LDP dilengkapi dengan Active Directory Administrative Tools. Untuk informasi selengkapnya, lihat Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola.

> **Note**
>
> Sebelum Anda menguji koneksi LDAPS, Anda harus menunggu hingga 30 menit untuk CA bawahan mengeluarkan sertifikat untuk pengendali domain Anda.

Untuk detail tambahan tentang LDAPS sisi server dan untuk melihat contoh kasus penggunaan tentang cara mengaturnya, lihat Cara Mengaktifkan LDAPS Sisi Server untuk Direktori Microsoft AD Terkelola Anda AWS di Blog Keamanan. AWS

Aktifkan LDAPS sisi klien menggunakan Microsoft AD yang Dikelola AWS

Dukungan Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) di Microsoft AD AWS Terkelola mengenkripsi komunikasi antara Microsoft Active Directory (AD) yang dikelola sendiri (lokal) dan aplikasi. AWS Contoh aplikasi tersebut termasuk WorkSpaces, AWS IAM Identity Center, Amazon QuickSight, dan Amazon Chime. Enkripsi ini membantu Anda melindungi data identitas organisasi dengan lebih baik dan memenuhi persyaratan keamanan Anda.

Prasyarat

Sebelum Anda mengaktifkan LDAPS sisi klien, Anda harus memenuhi persyaratan berikut.

Topik

- Buat hubungan kepercayaan antara Microsoft AD yang Dikelola dan AWS dikelola sendiri Microsoft Active Directory
- Men-deploy sertifikat server di Direktori Aktif
- Persyaratan sertifikat Otoritas Sertifikat
- Persyaratan jaringan

Buat hubungan kepercayaan antara Microsoft AD yang Dikelola dan AWS dikelola sendiri Microsoft Active Directory

Pertama, Anda perlu membangun hubungan kepercayaan antara Microsoft AD yang Dikelola dan AWS dikelola sendiri Microsoft Active Directory untuk mengaktifkan LDAPS sisi klien. Untuk informasi selengkapnya, lihat the section called “Menciptakan hubungan kepercayaan”.

Men-deploy sertifikat server di Direktori Aktif

Untuk mengaktifkan LDAPS sisi klien, Anda perlu untuk mendapatkan dan menginstal sertifikat server untuk setiap pengendali domain di Direktori Aktif. Sertifikat ini akan digunakan oleh layanan LDAP untuk mendengarkan dan secara otomatis menerima koneksi SSL dari klien LDAP. Anda dapat menggunakan sertifikat SSL yang dikeluarkan oleh deployment Active Directory Certificate Services (ADCS) atau dibeli dari penerbit komersial. Untuk informasi lebih lanjut tentang persyaratan sertifikat server Direktori Aktif, lihat LDAP melalui Sertifikat SSL (LDAPS) di situs web Microsoft.

Persyaratan sertifikat Otoritas Sertifikat

Sertifikat otoritas sertifikat (CA), yang mewakili penerbit sertifikat server Anda, diperlukan untuk operasi LDAPS sisi klien. Sertifikat CA cocok dengan sertifikat server yang disajikan oleh pengendali domain Direktori Aktif Anda untuk mengenkripsi komunikasi LDAP. Perhatikan persyaratan sertifikat CA berikut:

- Otoritas Sertifikasi Perusahaan (CA) diperlukan untuk mengaktifkan LDAPS sisi klien. Anda dapat menggunakan Layanan Active Directory Sertifikat, otoritas sertifikat komersial pihak ketiga, atau AWS Certificate Manager. Untuk informasi selengkapnya tentang Otoritas Sertifikat Microsoft Perusahaan, lihat Microsoftdokumentasi.
- Untuk mendaftarkan sertifikat, harus lebih dari 90 hari dari kedaluwarsa.
- Sertifikat harus dalam format Privacy Enhanced Mail (PEM). Jika mengekspor sertifikat CA dari dalam Direktori Aktif, pilih base64 encoded X.509 (.CER) sebagai format file ekspor.
- Maksimal lima (5) sertifikat CA dapat disimpan per direktori Microsoft AD yang AWS Dikelola.
- Sertifikat yang menggunakan algoritma tanda tangan RSASSA-PSS tidak didukung.
- Sertifikat CA yang berantai untuk setiap sertifikat server di setiap domain terpercaya harus terdaftar.

Persyaratan jaringan

AWS lalu lintas aplikasi LDAP akan berjalan secara eksklusif pada port TCP 636, tanpa fallback ke port LDAP 389. Namun, komunikasi Windows LDAP yang mendukung replikasi, kepercayaan, dan banyak lagi akan terus menggunakan LDAP port 389 dengan keamanan native Windows. Konfigurasikan grup AWS keamanan dan firewall jaringan untuk mengizinkan komunikasi TCP pada port 636 di AWS Microsoft AD Terkelola (keluar) dan Direktori Aktif yang dikelola sendiri (masuk). Biarkan port 389 LDAP terbuka antara Microsoft AD yang Dikelola AWS dan Direktori Aktif yang dikelola sendiri.

Aktifkan LDAPS sisi klien

Untuk mengaktifkan LDAPS sisi klien, Anda mengimpor sertifikat otoritas (CA) sertifikat ke Microsoft AD yang Dikelola AWS , dan kemudian mengaktifkan LDAPS pada direktori Anda. Setelah mengaktifkan, semua lalu lintas LDAP antara aplikasi AWS dan Direktori Aktif Anda akan mengalir dengan enkripsi saluran Lapisan Socket Aman (SSL).

Anda dapat menggunakan dua metode yang berbeda untuk mengaktifkan LDAPS sisi klien untuk direktori Anda. Anda dapat menggunakan AWS Management Console metode atau AWS CLI metode.

> **Note**
>
> LDAPS Sisi Klien adalah fitur Regional dari Microsoft AD yang Dikelola AWS . Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Topik

Langkah 1: Daftarkan sertifikat di AWS Directory Service

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat AWS Directory Service.

Metode 1: Untuk mendaftarkan sertifikat Anda di AWS Directory Service (AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mendaftarkan sertifikat Anda, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih menu Tindakan, lalu pilih Mendaftarkan sertifikat.
5. Di kotak dialog Daftarkan sertifikat CA, pilih Telusuri, lalu pilih sertifikat dan pilih Buka.
6. Pilih Daftarkan sertifikat.

Metode 2: Untuk mendaftarkan sertifikat Anda di AWS Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk data sertifikat, arahkan ke lokasi file sertifikat CA Anda. ID sertifikat akan diberikan dalam tanggapan.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Langkah 2: Periksa status pendaftaran

Untuk melihat status pendaftaran sertifikat atau daftar sertifikat terdaftar, gunakan salah satu metode berikut:

Metode 1: Untuk memeriksa status pendaftaran sertifikat di AWS Directory Service (AWS Management Console)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Meninjau status pendaftaran sertifikat saat ini yang ditampilkan di bawah kolom Status pendaftaran. Ketika nilai status pendaftaran berubah menjadi Registered, sertifikat Anda telah berhasil didaftarkan.

Metode 2: Untuk memeriksa status pendaftaran sertifikat di AWS Directory Service (AWS CLI)

- Jalankan perintah berikut. Jika nilai status mengembalikan `Registered`, sertifikat Anda telah berhasil didaftarkan.

```
aws ds list-certificates --directory-id your_directory_id
```

Langkah 3: Aktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk mengaktifkan LDAPS sisi klien masuk. AWS Directory Service

> **Note**
>
> Anda harus berhasil mendaftarkan setidaknya satu sertifikat sebelum Anda dapat mengaktifkan LDAPS sisi klien.

Metode 1: Untuk mengaktifkan LDAPS sisi klien di () AWS Directory ServiceAWS Management Console

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Pilih Aktifkan. Jika opsi ini tidak tersedia, verifikasi bahwa sertifikat yang valid telah berhasil terdaftar, dan kemudian coba lagi.
3. Di kotak dialog Aktifkan LDAPS sisi klien, pilih Aktifkan.

Metode 2: Untuk mengaktifkan LDAPS sisi klien di () AWS Directory ServiceAWS CLI

- Jalankan perintah berikut.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Langkah 4: Periksa status LDAPS

Gunakan salah satu metode berikut untuk memeriksa status LDAPS di. AWS Directory Service

Metode 1: Untuk memeriksa status LDAPS di AWS Directory Service ()AWS Management Console

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Jika nilai status ditampilkan sebagai Diaktifkan, LDAPS telah berhasil dikonfigurasi.

Metode 2: Untuk memeriksa status LDAPS di AWS Directory Service ()AWS CLI

- Jalankan perintah berikut. Jika nilai status mengembalikan `Enabled`, LDAPS telah berhasil dikonfigurasi.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Mengelola LDAPS sisi klien

Gunakan perintah ini untuk mengelola konfigurasi LDAPS Anda.

Anda dapat menggunakan dua metode yang berbeda untuk mengelola pengaturan LDAPS sisi klien. Anda dapat menggunakan AWS Management Console metode atau AWS CLI metode.

Melihat detail sertifikat

Gunakan salah satu metode berikut untuk melihat ketika sertifikat diatur untuk kedaluwarsa.

Metode 1: Untuk melihat detail sertifikat di AWS Directory Service (AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region di mana Anda ingin melihat sertifikat, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, di bawah Sertifikat CA, informasi tentang sertifikat akan ditampilkan.

Metode 2: Untuk melihat detail sertifikat di AWS Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Membatalkan pendaftaran sertifikat

Gunakan salah satu metode berikut untuk membatalkan pendaftaran sertifikat.

> **Note**
>
> Jika hanya satu sertifikat yang terdaftar, Anda harus terlebih dahulu menonaktifkan LDAPS sebelum Anda dapat membatalkan pendaftaran sertifikat.

Metode 1: Untuk membatalkan pendaftaran sertifikat di () AWS Directory ServiceAWS Management Console

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin membatalkan pedaftaran sertifikat Anda, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih Tindakan, lalu pilih Membatalkan pendaftaran sertifikat.
5. Di kotak dialog Membatalkan pendaftaran sertifikat CA, pilih Batalkan pendaftaran.

Metode 2: Untuk membatalkan pendaftaran sertifikat di () AWS Directory ServiceAWS CLI

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Menonaktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk menonaktifkan LDAPS sisi klien.

Metode 1: Untuk menonaktifkan LDAPS sisi klien di () AWS Directory ServiceAWS Management Console

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menonaktifkan LDAPS sisi klien, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.

- Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.

4. Di bagian LDAPS sisi klien, pilih Nonaktifkan.
5. Di kotak dialog Nonaktifkan LDAPS sisi klien, pilih Nonaktifkan.

Metode 2: Untuk menonaktifkan LDAPS sisi klien di () AWS Directory ServiceAWS CLI

- Jalankan perintah berikut.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Masalah pendaftaran sertifikat

Proses untuk mendaftarkan pengontrol domain Microsoft AD AWS Terkelola dengan sertifikat CA dapat memakan waktu hingga 30 menit. Jika Anda mengalami masalah dengan pendaftaran sertifikat dan ingin memulai ulang pengontrol domain AWS Microsoft AD Terkelola, Anda dapat menghubungi. AWS Support Untuk membuat kasus dukungan, lihat Membuat kasus dukungan dan manajemen kasus.

Mengelola kepatuhan untuk Microsoft AD yang Dikelola AWS

Anda dapat menggunakan Microsoft AD yang Dikelola AWS untuk mendukung aplikasi sadar Direktori Aktif, di Cloud AWS, yang tunduk pada persyaratan kepatuhan berikut. Namun, aplikasi Anda tidak akan mematuhi persyaratan kepatuhan jika Anda menggunakan Simple AD.

Standar kepatuhan yang didukung

Microsoft AD yang Dikelola AWS telah menjalani audit untuk standar berikut dan memenuhi syarat untuk digunakan sebagai bagian dari solusi yang Anda butuhkan untuk mendapatkan sertifikasi kepatuhan.

Microsoft AD yang Dikelola AWS memenuhi persyaratan keamanan Federal Risk and Authorization Management Program (FedRAMP) dan telah menerima FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) di Baseline Sedang dan Tinggi FedRAMP. Untuk informasi selengkapnya tentang FedRAMP, lihat Kepatuhan FedRAMP.

Microsoft AD yang Dikelola AWS memiliki pengesahan kepatuhan untuk Standar Keamanan Data (DSS) Payment Card Industry (PCI) versi 3.2 pada Penyedia Layanan Level 1. Pelanggan yang menggunakan produk AWS dan layanan untuk menyimpan, memproses, atau mengirimkan data pemegang kartu dapat menggunakan Microsoft AD yang Dikelola AWS karena mereka mengelola sertifikasi kepatuhan PCI DSS mereka sendiri.

Untuk informasi lebih lanjut tentang PCI DSS, termasuk cara meminta salinan dari Paket Kepatuhan PCI AWS, lihat PCI DSS Level 1. Yang penting, Anda harus mengkonfigurasi kebijakan kata sandi terperinci di Microsoft AD yang Dikelola AWS untuk konsisten dengan PCI DSS versi 3.2 standar. Untuk detail tentang kebijakan mana yang harus diberlakukan, lihat bagian di bawah ini yang berjudul Aktifkan Kepatuhan PCI untuk Direktori Microsoft AD yang Dikelola AWS Anda.

AWS telah melebarkan program kepatuhan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) untuk menyertakan Microsoft AD yang Dikelola AWS sebagai Layanan yang memenuhi syarat HIPAA. Jika Anda memiliki Perjanjian Rekan Bisnis (BAA) yang dieksekusi dengan AWS, Anda dapat menggunakan Microsoft AD yang Dikelola AWS untuk membantu membangun aplikasi patuh HIPAA Anda.

AWS menawarkan Laporan resmi yang berfokus pada HIPAAbagi pelanggan yang tertarik untuk mempelajari lebih lanjut tentang bagaimana mereka dapat memanfaatkan AWS untuk pengolahan dan penyimpanan informasi kesehatan. Untuk informasi selengkapnya, lihat Kepatuhan HIPAA.

Tanggung Jawab Bersama

Keamanan, termasuk kepatuhan FedRAMP, HIPAA, dan PCI, adalah tanggung jawab bersama. Penting untuk memahami bahwa status kepatuhan Microsoft AD yang Dikelola AWS tidak secara otomatis berlaku untuk aplikasi yang Anda jalankan di Cloud AWS. Anda perlu memastikan bahwa penggunaan layanan AWS Anda sesuai dengan standar.

Untuk daftar lengkap berbagai program kepatuhan AWS yang didukung Microsoft AD yang Dikelola AWS, lihat layanan AWS dalam lingkup oleh program kepatuhan.

Aktifkan kepatuhan PCI untuk direktori Microsoft AD yang Dikelola AWS Anda.

Untuk mengaktifkan direktori Microsoft AD yang Dikelola AWS Anda, Anda harus mengkonfigurasi kebijakan kata sandi terperinci seperti yang ditentukan dalam Pengesahan Kepatuhan (AOC) PCI DSS dan dokumen Ringkasan Tanggung Jawab yang disediakan oleh AWS Artifact.

Untuk informasi selengkapnya tentang menggunakan kebijakan kata sandi terperinci, lihat Mengelola kebijakan kata sandi untuk Microsoft AD yang AWS Dikelola.

Meningkatkan konfigurasi keamanan jaringan Microsoft AD yang Dikelola AWS Anda

Grup keamanan AWS yang disediakan untuk direktori Microsoft AD yang Dikelola AWS dikonfigurasi dengan port jaringan inbound minimum yang diperlukan untuk mendukung semua kasus penggunaan

yang diketahui untuk direktori Microsoft AD yang Dikelola AWS Anda. Untuk informasi selengkapnya pada Grup Keamanan yang disediakan AWS, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.

Untuk lebih meningkatkan keamanan jaringan dari direktori Microsoft AD yang Dikelola AWS Anda dapat memodifikasi Grup Keamanan AWS berdasarkan skenario umum yang tercantum di bawah ini.

Topik

Aplikasi AWS hanya mendukung

Semua akun pengguna disediakan hanya di Microsoft AD yang Dikelola AWS untuk digunakan dengan aplikasi AWS yang mendukung, seperti berikut:

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

Anda dapat menggunakan konfigurasi Grup Keamanan AWS berikut untuk memblokir semua lalu lintas non-esensial ke pengendali domain Microsoft AD yang Dikelola AWS.

> **Note**
>
> - Berikut ini yang tidak kompatibel dengan konfigurasi Grup Keamanan AWS ini:
>   - Instans Amazon EC2

- Amazon FSx
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- WorkSpaces
- Kepercayaan Direktori Aktif
- Domain bergabung klien atau server

Aturan Masuk

Tidak ada.

Aturan Outbound

Tidak ada.

Aplikasi AWS hanya dengan dukungan kepercayaan

Semua akun pengguna disediakan di Microsoft AD yang Dikelola AWS atau Direktori Aktif terpercaya untuk digunakan dengan aplikasi AWS yang mendukung, seperti berikut:

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

Anda dapat memodifikasi konfigurasi Grup Keamanan AWS yang disediakan untuk memblokir semua lalu lintas non-esensial ke pengendali domain Microsoft AD yang Dikelola AWS.

Note

- Berikut ini yang tidak kompatibel dengan konfigurasi Grup Keamanan AWS ini:
  - Instans Amazon EC2
  - Amazon FSx
  - Amazon RDS for MySQL
  - Amazon RDS for Oracle
  - Amazon RDS for PostgreSQL
  - Amazon RDS for SQL Server
  - WorkSpaces
  - Kepercayaan Direktori Aktif
  - Domain bergabung klien atau server
- Konfigurasi ini mengharuskan Anda untuk memastikan jaringan “CIDR lokal” aman.
- TCP 445 digunakan untuk pembuatan kepercayaan saja dan dapat dihapus setelah kepercayaan telah ditetapkan.
- TCP 636 hanya diperlukan ketika LDAP atas SSL sedang digunakan.

Aturan Masuk

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	CIDR di tempat	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	CIDR di tempat	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	389	CIDR di tempat	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP & UDP	464	CIDR di tempat	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentikasi komputer, kepercayaan
TCP	445	CIDR di tempat	SMB / CIFS	Replikasi, autentikasi pengguna dan komputer, kepercayaan kebijakan grup
TCP	135	CIDR di tempat	Replikasi	RPC, EPM
TCP	636	CIDR di tempat	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	49152 - 65535	CIDR di tempat	RPC	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	CIDR di tempat	LDAP GC & LDAP GC SSL	Direktori, replikasi, kebijakan pengguna dan grup autentikasi komputer, kepercayaan
UDP	123	CIDR di tempat	Waktu Windows	Waktu Windows, kepercayaan

Aturan Outbound

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
Semua	Semua	CIDR di tempat	Semua Lalu lintas	

Dukungan aplikasi AWS dan beban kerja Direktori Aktif asli

Akun pengguna disediakan hanya di Microsoft AD yang Dikelola AWS untuk digunakan dengan aplikasi AWS yang mendukung, seperti berikut:

- Amazon Chime
- Amazon Connect

- Instans Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Anda dapat memodifikasi konfigurasi Grup Keamanan AWS yang disediakan untuk memblokir semua lalu lintas non-esensial ke pengendali domain Microsoft AD yang Dikelola AWS.

> **Note**
>
> - Trust Active Directory tidak dapat dibuat dan AWS dikelola antara direktori AD Microsoft Terkelola dan domain lokal.
> - Hal ini mengharuskan Anda untuk memastikan bahwa jaringan “Client CIDR” aman.
> - TCP 636 hanya diperlukan ketika LDAP atas SSL sedang digunakan.
> - Jika Anda ingin menggunakan Enterprise CA dengan konfigurasi ini Anda perlu membuat aturan keluar “TCP, 443, CA CIDR”.

Aturan Masuk

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	Client CIDR	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	Client CIDR	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	Client CIDR	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP & UDP	445	Client CIDR	SMB / CIFS	Replikasi, autentikasi pengguna dan komputer, kepercayaan kebijakan grup
TCP & UDP	464	Client CIDR	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentika si komputer, kepercayaan
TCP	135	Client CIDR	Replikasi	RPC, EPM

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	636	Client CIDR	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP	49152 - 65535	Client CIDR	RPC	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	Client CIDR	LDAP GC & LDAP GC SSL	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP	9389	Client CIDR	SOAP	Layanan web AD DS
UDP	123	Client CIDR	Waktu Windows	Waktu Windows, kepercayaan
UDP	138	Client CIDR	DFSN & NetLogon	DFS, kebijakan grup

Aturan Outbound

Tidak ada.

Dukungan aplikasi AWS dan beban kerja Direktori Aktif asli dengan dukungan kepercayaan

Semua akun pengguna disediakan di Microsoft AD yang Dikelola AWS atau Direktori Aktif terpercaya untuk digunakan dengan aplikasi AWS yang mendukung, seperti berikut:

- Amazon Chime
- Amazon Connect
- Instans Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Anda dapat memodifikasi konfigurasi Grup Keamanan AWS yang disediakan untuk memblokir semua lalu lintas non-esensial ke pengendali domain Microsoft AD yang Dikelola AWS.

> **Note**
>
> - Ini mengharuskan Anda untuk memastikan jaringan “CIDR lokal” dan “CIDR Klien” aman.
> - TCP 445 dengan “CIDR lokal” digunakan untuk pembuatan kepercayaan saja dan dapat dihapus setelah kepercayaan telah ditetapkan.
> - TCP 445 dengan “Client CIDR” harus dibiarkan terbuka seperti yang diperlukan untuk pemrosesan Kebijakan Grup.
> - TCP 636 hanya diperlukan ketika LDAP atas SSL sedang digunakan.

- Jika Anda ingin menggunakan Enterprise CA dengan konfigurasi ini Anda perlu membuat aturan keluar “TCP, 443, CA CIDR”.

Aturan Masuk

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	CIDR di tempat	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	CIDR di tempat	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	CIDR di tempat	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP & UDP	464	CIDR di tempat	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentika si komputer, kepercayaan
TCP	445	CIDR di tempat	SMB / CIFS	Replikasi, autentikasi pengguna

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
				dan komputer, kepercayaan kebijakan grup
TCP	135	CIDR di tempat	Replikasi	RPC, EPM
TCP	636	CIDR di tempat	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP	49152 - 65535	CIDR di tempat	RPC	Replikasi, pengguna dan autentika si komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	CIDR di tempat	LDAP GC & LDAP GC SSL	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
UDP	123	CIDR di tempat	Waktu Windows	Waktu Windows, kepercayaan

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP & UDP	53	Client CIDR	DNS	Autentikasi pengguna dan komputer, resolusi nama, kepercayaan
TCP & UDP	88	Client CIDR	Kerberos	Autentikasi pengguna dan komputer, kepercayaan tingkat forest
TCP & UDP	389	Client CIDR	LDAP	Direktori , replikasi , kebijakan pengguna dan grup autentika si komputer, kepercayaan
TCP & UDP	445	Client CIDR	SMB / CIFS	Replikasi, autentikasi pengguna dan komputer, kepercayaan kebijakan grup
TCP & UDP	464	Client CIDR	Kerberos mengubah / mengatur kata sandi	Replikasi, pengguna dan autentika si komputer, kepercayaan
TCP	135	Client CIDR	Replikasi	RPC, EPM

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
TCP	636	Client CIDR	LDAP SSL	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP	49152 - 65535	Client CIDR	RPC	Replikasi, pengguna dan autentikasi komputer, kebijakan grup, kepercayaan
TCP	3268 - 3269	Client CIDR	LDAP GC & LDAP GC SSL	Direktori , replikasi , kebijakan pengguna dan grup autentikasi komputer, kepercayaan
TCP	9389	Client CIDR	SOAP	Layanan web AD DS
UDP	123	Client CIDR	Waktu Windows	Waktu Windows, kepercayaan
UDP	138	Client CIDR	DFSN & NetLogon	DFS, kebijakan grup

Aturan Outbound

Protokol	Rentang Port	Sumber	Jenis lalu lintas	Penggunaan Direktori Aktif
Semua	Semua	CIDR di tempat	Semua Lalu lintas	

Konfigurasikan pengaturan keamanan direktori

Anda dapat mengonfigurasi setelan direktori berbutir halus untuk AWS Microsoft AD yang Dikelola agar memenuhi persyaratan kepatuhan dan keamanan tanpa peningkatan beban kerja operasional. Dalam pengaturan direktori, Anda dapat memperbarui konfigurasi saluran aman untuk protokol dan cipher yang digunakan dalam direktori Anda. Misalnya, Anda memiliki fleksibilitas untuk menonaktifkan cipher warisan individu, seperti RC4 atau DES, dan protokol, seperti SSL 2.0/3.0 dan TLS 1.0/1.1. AWS Microsoft AD yang dikelola kemudian menyebarkan konfigurasi ke semua pengontrol domain di direktori Anda, mengelola reboot pengontrol domain, dan mempertahankan konfigurasi ini saat Anda meningkatkan skala atau menerapkan tambahan. Wilayah AWS Untuk semua pengaturan yang tersedia, lihatDaftar pengaturan keamanan direktori.

Edit pengaturan keamanan direktori

Anda dapat mengonfigurasi dan mengedit pengaturan untuk direktori mana pun.

Untuk mengedit pengaturan direktori

1. Masuk ke AWS Management Console dan buka konsol AWS Directory Service dihttps://console.aws.amazon.com/directoryservicev2/.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah Jaringan & keamanan, temukan pengaturan Direktori, lalu pilih Edit pengaturan.
4. Di Pengaturan Edit, ubah Nilai untuk pengaturan yang ingin Anda edit. Saat Anda mengedit setelan, statusnya berubah dari Default menjadi Siap untuk Diperbarui. Jika Anda telah mengedit pengaturan sebelumnya, statusnya berubah dari Diperbarui menjadi Siap untuk Diperbarui. Kemudian, pilih Review.
5. Di Pengaturan tinjauan dan perbarui, lihat Pengaturan direktori dan pastikan bahwa semua nilai baru sudah benar. Jika Anda ingin membuat perubahan lain pada pengaturan Anda, pilih Edit pengaturan. Jika Anda puas dengan perubahan dan siap menerapkan nilai baru, pilih Perbarui pengaturan. Kemudian, Anda dibawa kembali ke halaman ID direktori.

> **Note**
>
> Di bawah Pengaturan direktori, Anda dapat melihat Status pengaturan yang diperbarui. Saat pengaturan diimplementasikan, Status menampilkan Memperbarui. Anda tidak dapat mengedit pengaturan lain saat pengaturan menampilkan Memperbarui di bawah Status. Status menampilkan Diperbarui jika pengaturan berhasil diperbarui dengan pengeditan Anda. Status ditampilkan Gagal jika pengaturan gagal diperbarui dengan pengeditan Anda.

Pengaturan keamanan direktori gagal

Jika terjadi kesalahan selama pembaruan pengaturan, Status ditampilkan sebagai Gagal. Dalam status gagal, pengaturan tidak diperbarui ke nilai baru, dan nilai asli tetap diterapkan. Anda dapat mencoba lagi memperbarui pengaturan ini atau mengembalikannya ke nilai sebelumnya.

Untuk mengatasi setelan yang diperbarui gagal

- Di bawah Pengaturan direktori, pilih Selesaikan setelan yang gagal. Kemudian, lakukan salah satu hal berikut:
  - Untuk mengembalikan setelan Anda kembali ke nilai aslinya sebelum status kegagalan, pilih Kembalikan setelan yang gagal. Kemudian, pilih Kembalikan di modal pop-up.
  - Untuk mencoba lagi memperbarui pengaturan direktori Anda, pilih Coba lagi setelan yang gagal. Jika Anda ingin membuat perubahan tambahan pada pengaturan direktori Anda sebelum mencoba kembali pembaruan yang gagal, pilih Lanjutkan pengeditan. Pada Tinjau dan coba lagi pembaruan yang gagal, pilih Pengaturan pembaruan.

Daftar pengaturan keamanan direktori

Daftar berikut menunjukkan jenis, nama setelan, nama API, nilai potensial, dan deskripsi setelan untuk semua setelan keamanan direktori yang tersedia.

TLS 1.2 dan AES 256/256 adalah pengaturan keamanan direktori default jika semua pengaturan keamanan lainnya dinonaktifkan. Mereka tidak bisa dinonaktifkan.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
Otentikas i Berbasis Sertifikat	Komper i Backdat g Sertifika t	CERTIFICA TE_BACKDA TING_COMP ENSATION	Tahun: 0 hingga 50 Bulan: 0 hingga 11 Hari: 0 hingga 30 Jam: 0 hingga 23 Menit: 0 hingga 59 Detik: 0 hingga 59	Tentukan nilai untuk menunjukkan lamanya waktu sertifikat dapat mendahulu i pengguna di Active Directory dan masih digunakan untuk otentikas i di Active Directory. Nilai default adalah 10 menit. Anda dapat mengatur nilai ini dari 1 detik hingga 50 tahun. Untuk mengonfigurasi pengaturan ini, Anda harus memilih jenis Kompatibi litas untuk Strong Certifica te Binding Enforcement.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
				Untuk informasi selengkap nya, lihat KB5014754 —Perubaha n autentika si berbasis sertifikat pada pengontro l domain Windows di dokumenta si Dukungan Microsoft.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	Sertifika t Penega Kuat	CERTIFICA TE_STRONG _ENFORCEM ENT	Kompatibilitas, Penegakan Penuh	Tentukan salah satu dari jenis penegakan berikut: • Kompatibi litas (default) : Otentikas i diperbole hkan jika sertifikat tidak dapat dipetakan dengan kuat ke pengguna. Jika sertifika t mendahulu i akun pengguna di Active Directory , Anda juga harus menetapka n Certificate Backdating Compensat ion, atau otentikasi akan gagal. • Penegakan Penuh:

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
				Otentikas i tidak diizinkan jika sertifika t tidak dapat dipetakan dengan kuat ke pengguna. Jika Anda memilih jenis penegakan ini, Kompensas i Backdatin g Sertifikat tidak dapat dikonfigurasi. Untuk informasi selengkap nya, lihat KB5014754 —Perubaha n autentika si berbasis sertifikat pada pengontro l domain Windows di dokumenta

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
				si Dukungan Microsoft.
Saluran Aman: Cipher	AES 128/128	AES_128_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an cipher enkripsi AES 128/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.
	DES 56/56	DES_56_56	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi DES 56/56 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	RC2 40/128	RC2_40_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC2 40/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.
	RC2 56/128	RC2_56_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC2 56/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	RC2 128/128	RC2_128_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC2 128/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.
	RC4 40/128	RC4_40_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC4 40/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	RC4 56/128	RC4_56_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC4 56/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.
	RC4 64/128	RC4_64_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC4 64/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	RC4 128/128	RC4_128_128	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifk an sandi enkripsi RC4 128/128 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.
	Tiga DES 168/168	3DES_168_ 168	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan sandi enkripsi Triple DES 168/168 untuk komunikas i saluran aman antara pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
Saluran Aman: Protokol	PCT 1.0	PCT_1_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol PCT 1.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.
	SSL 2.0	SSL_2_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol SSL 2.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	SSL 3.0	SSL_3_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol SSL 3.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.
	TLS 1.0	TLS_1_0	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol TLS 1.0 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.

Tipe	Nama pengatu n	Nama API	Nilai potensial	Deskripsi pengaturan
	TLS 1.1	TLS_1_1	Aktifkan, Nonaktifkan	Aktifkan atau nonaktifkan protokol TLS 1.1 untuk komunikasi saluran aman (Server dan Klien) pada pengontro l domain di direktori Anda.

Siapkan AWS Private CA Konektor untuk AD

Anda dapat mengintegrasikan Microsoft AD yang AWS Dikelola dengan AWS Private Certificate Authority (CA) untuk menerbitkan dan mengelola sertifikat bagi pengguna, grup, dan mesin yang bergabung dengan domain Direktori Aktif. AWS Private CA Connector for Active Directory memungkinkan Anda menggunakan pengganti AWS Private CA drop-in yang dikelola sepenuhnya untuk CA perusahaan yang dikelola sendiri tanpa perlu menyebarkan, menambal, atau memperbarui agen lokal atau server proxy.

> **Note**
>
> Pendaftaran sertifikat LDAPS sisi server untuk pengontrol domain AWS Microsoft AD Terkelola dengan AWS Private CA Konektor untuk Direktori Aktif tidak didukung. Untuk mengaktifkan LDAPS sisi server untuk direktori Anda, lihat Cara mengaktifkan LDAPS sisi server untuk direktori Microsoft AD yang Dikelola. AWS

Anda dapat mengatur AWS Private CA integrasi dengan direktori Anda melalui konsol Directory Service, konsol AWS Private CA Connector for Active Directory, atau dengan memanggil `CreateTemplate`API. Untuk mengatur integrasi Private CA melalui konsol AWS Private CA

Connector for Active Directory, lihat Membuat template konektor. Lihat di bawah untuk langkah-langkah tentang cara mengatur integrasi ini dari AWS Directory Service konsol.

Untuk mengatur AWS Private CA Konektor untuk AD

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol dihttps://console.aws.amazon.com/directoryservicev2/.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah tab Jaringan & Keamanan, di bawah AWS Private CA Konektor untuk AD, pilih Siapkan AWS Private CA Konektor untuk AD. Halaman Buat sertifikat CA Pribadi untuk Active Directory muncul. Ikuti langkah-langkah di konsol untuk membuat CA Pribadi Anda untuk Active Directory konektor untuk mendaftar dengan CA Pribadi Anda. Untuk informasi selengkapnya, lihat Membuat konektor.
4. Setelah membuat konektor, ikuti langkah-langkah di bawah ini untuk melihat detail, termasuk status konektor dan status Private CA terkait.

Untuk melihat AWS Private CA Konektor untuk AD

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol dihttps://console.aws.amazon.com/directoryservicev2/.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah Jaringan & Keamanan, di bawah AWS Private CA Konektor untuk AD, Anda dapat melihat konektor CA Pribadi dan CA Pribadi terkait. Secara default, Anda melihat bidang berikut:

    a. AWS Private CA Connector ID — Pengidentifikasi unik untuk AWS Private CA konektor. Mengkliknya mengarah ke halaman detail AWS Private CA konektor itu.
    b. AWS Private CA subjek — Informasi tentang nama yang dibedakan untuk CA. Mengkliknya mengarah ke halaman detail itu AWS Private CA.
    c. Status - Berdasarkan pemeriksaan status untuk AWS Private CA Konektor dan AWS Private CA. Jika kedua pemeriksaan lulus, Active akan ditampilkan. Jika salah satu pemeriksaan gagal, 1/2 pemeriksaan gagal ditampilkan. Jika kedua pemeriksaan gagal, Gagal ditampilkan. Untuk informasi selengkapnya tentang status gagal, arahkan kursor ke hyperlink untuk mengetahui pemeriksaan mana yang gagal. Ikuti instruksi di konsol untuk memulihkan.
    d. Tanggal dibuat - Hari AWS Private CA Konektor dibuat.

Untuk informasi selengkapnya, lihat Lihat detail konektor.

Memantau Microsoft AD yang Dikelola AWS Anda

Anda dapat memantau direktori Microsoft AD yang Dikelola AWS Anda dengan metode berikut:

Topik

- Memahami status direktori Anda
- Konfigurasikan pemberitahuan status direktori dengan Amazon SNS
- Meninjau log direktori Microsoft AD yang Dikelola AWS Anda
- Mengaktifkan penerusan log
- Pantau pengontrol domain Anda dengan metrik kinerja

Memahami status direktori Anda

Berikut ini adalah berbagai status untuk direktori.

Aktif

Direktori beroperasi secara normal. Tidak ada masalah yang terdeteksi oleh AWS Directory Service untuk direktori Anda.

Creating

Direktori saat ini sedang dibuat. Pembuatan direktori biasanya memakan waktu antara 20 sampai 45 menit tetapi dapat bervariasi tergantung pada beban sistem.

Dihapus

Direktori telah dihapus. Semua sumber daya untuk direktori telah dirilis. Setelah direktori memasuki keadaan ini, direktori tidak dapat dipulihkan.

Deleting

Direktori saat ini sedang dihapus. Direktori akan tetap dalam keadaan ini sampai benar-benar dihapus. Setelah direktori memasuki keadaan ini, operasi hapus tidak dapat dibatalkan, dan direktori tidak dapat dipulihkan.

Failed

Direktori tidak dapat dibuat. Harap hapus direktori ini. Jika masalah ini berlanjut, hubungi PusatAWS Support.

Terganggu

Direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh. Terdapat banyak potensi alasan untuk keadaan direktori seperti ini. Ini termasuk aktivitas pemeliharaan operasional normal seperti patching atau rotasi instans EC2, hot spotting sementara oleh aplikasi pada salah satu pengendali domain Anda, atau perubahan yang Anda buat ke jaringan Anda yang secara tidak sengaja mengganggu komunikasi direktori. Untuk informasi selengkapnya, lihat salah satu dari Pemecahan Masalah AWS Microsoft AD yang Dikelola, Memecahkan masalah AD Connector, Pemecahan masalah Simple AD. Untuk masalah terkait pemeliharaan normal, AWS selesaikan masalah ini dalam waktu 40 menit. Jika setelah meninjau topik pemecahan masalah, direktori Anda dalam keadaan Terganggu lebih dari 40 menit, kami merekomendasikan Anda untuk menghubungi PusatAWS Support.

> **Important**
>
> Jangan memulihkan snapshot ketika direktori dalam keadaan Terganggu. Sangatlah jarang pemulihan snapshot diperlukan untuk mengatasi gangguan. Untuk informasi selengkapnya, lihat Snapshot atau pulihkan direktori Anda.

Tidak bisa dioperasikan

Direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.

Diminta

Permintaan untuk membuat direktori Anda sedang tertunda.

RestoreFailed

Memulihkan direktori dari snapshot gagal. Silakan coba lagi operasi pemulihan. Jika ini berlanjut, cobalah snapshot yang berbeda, atau hubungi AWS Support Pusat.

Memulihkan

Direktori saat ini sedang dipulihkan dari snapshot otomatis atau manual. Memulihkan dari snapshot biasanya memakan waktu beberapa menit, tergantung pada ukuran data direktori dalam snapshot.

Konfigurasikan pemberitahuan status direktori dengan Amazon SNS

Menggunakan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) saat status direktori Anda berubah. Anda akan diberitahu jika direktori Anda berubah dari status Aktif ke status Terganggu atau Tidak dapat dioperasikan. Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Cara Kerjanya

Amazon SNS menggunakan “topik” untuk mengumpulkan dan mendistribusikan pesan. Setiap topik memiliki satu atau lebih pelanggan yang menerima pesan yang telah diterbitkan untuk topik tersebut. Dengan menggunakan langkah-langkah di bawah ini, Anda dapat menambahkan AWS Directory Service sebagai penerbit ke topik Amazon SNS. Saat AWS Directory Service mendeteksi perubahan dalam status direktori Anda, ia menerbitkan pesan ke topik tersebut, yang kemudian dikirim ke pelanggan topik tersebut.

Anda dapat mengaitkan beberapa direktori sebagai penerbit ke satu topik. Anda juga dapat menambahkan pesan status direktori ke topik yang sebelumnya Anda buat di Amazon SNS. Anda memiliki kendali terperinci atas siapa yang dapat menerbitkan dan berlangganan topik. Untuk informasi lengkap tentang Amazon SNS, lihat Apa yang Dimaksud dengan Amazon SNS?.

> **Note**
>
> Pemberitahuan status direktori adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk mengaktifkan olahpesan SNS untuk direktori Anda

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan olahpesan SNS, lalu pilih tab Pemeliharaan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pemeliharaan.

4. Di bagian Pemantauan direktori, pilih Tindakan, dan kemudian pilih Buat notifikasi.
5. Pada halaman Buat notifikasi, pilih Pilih jenis notifikasi, lalu pilih Buat notifikasi baru. Atau, jika Anda sudah memiliki topik SNS yang ada, Anda dapat memilih Mengasosiasikan topik SNS yang ada untuk mengirim pesan status dari direktori ini ke topik tersebut.

> **Note**
>
> Jika Anda memilih Buat notifikasi baru tetapi kemudian menggunakan nama topik yang sama untuk topik SNS yang sudah ada, Amazon SNS tidak membuat topik baru, tetapi hanya menambahkan informasi langganan baru ke topik yang ada.
> Jika Anda memilih Mengasosiasikan topik SNS yang ada, Anda hanya akan dapat memilih topik SNS yang ada di Region yang sama dengan direktori.

6. Pilih Jenis penerima dan masukkan informasi kontak Penerima. Jika Anda memasukkan nomor telepon untuk SMS, gunakan angka saja. Jangan menyertakan tanda hubung, spasi, atau tanda kurung.
7. (Opsional) Berikan nama untuk topik Anda dan nama tampilan SNS. Nama tampilan adalah nama pendek hingga 10 karakter yang disertakan dalam semua pesan SMS dari topik ini. Bila menggunakan opsi SMS, nama tampilan diperlukan.

> **Note**
>
> Jika Anda masuk menggunakan pengguna IAM atau peran yang hanya memiliki kebijakan DirectoryServiceFullAccessterkelola, nama topik Anda harus dimulai dengan “DirectoryMonitoring”. Jika Anda ingin menyesuaikan nama topik Anda lebih lanjut, Anda memerlukan hak istimewa tambahan untuk SNS.

8. Pilih Buat.

Jika Anda ingin menunjuk pelanggan SNS tambahan, seperti alamat email tambahan, antrian Amazon SQS AWS Lambdaatau, Anda dapat melakukan ini dari konsol Amazon SNS.

Untuk menghapus pesan status direktori dari topik

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:

- Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menghapus pesan status, lalu pilih tab Pemeliharaan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
- Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pemeliharaan.

4. Di bagian Pemantauan direktori, pilih nama topik SNS dalam daftar, pilih Tindakan, dan kemudian pilih Hapus.
5. Pilih Hapus.

Ini akan menghapus direktori Anda sebagai penerbit untuk topik SNS yang dipilih. Jika Anda ingin menghapus seluruh topik, Anda dapat melakukan ini dari konsol Amazon SNS.

> **Note**
>
> Sebelum menghapus topik Amazon SNS menggunakan konsol SNS, Anda harus memastikan bahwa direktori tidak mengirim pesan status untuk topik tersebut.
> Jika Anda menghapus topik Amazon SNS menggunakan konsol SNS, perubahan ini tidak akan segera tercermin dalam konsol Directory Service. Anda hanya akan diberitahu pada saat direktori menerbitkan notifikasi untuk topik yang dihapus, dalam hal ini Anda akan melihat status diperbarui pada tab Pemantauan direktori yang menunjukkan topik tidak dapat ditemukan.
> Oleh karena itu, untuk menghindari kehilangan pesan status direktori penting, sebelum menghapus topik apa pun yang menerima pesan dari AWS Directory Service, kaitkan direktori Anda dengan topik Amazon SNS yang berbeda.

Meninjau log direktori Microsoft AD yang Dikelola AWS Anda

Log keamanan dari instans pengendali domain Microsoft AD yang Dikelola AWS diarsipkan selama satu tahun. Anda juga dapat mengkonfigurasi direktori Microsoft AD yang Dikelola AWS untuk meneruskan log pengendali domain ke Amazon CloudWatch Logs hampir secara real time. Untuk informasi selengkapnya, lihat Mengaktifkan penerusan log.

AWS mencatat peristiwa berikut untuk kepatuhan.

Kategori pemantauan	Pengaturan kebijakan	Status audit
Masuk akun	Audit Validasi Kredensial	Sukses, Gagal
	Audit Peristiwa Masuk Akun Lainnya	Sukses, Gagal
Pengelolaan Akun	Audit Pengelolaan Akun Komputer	Sukses, Gagal
	Audit Pengelolaan Akun Lainnya	Sukses, Gagal
	Audit Pengelolaan Grup Keamanan	Sukses, Gagal
	Audit Pengelolaan Akun Pengguna	Sukses, Gagal
Pelacakan terperinci	Audit Aktivitas DPAPI	Sukses, Gagal
	Audit Aktivitas PNP	Berhasil
	Audit Pembuatan Proses	Sukses, Gagal
Akses DS	Audit Akses Directory Service	Sukses, Gagal
	Audit Perubahan Directory Service	Sukses, Gagal
Masuk/Keluar	Audit Penguncian Akun	Sukses, Gagal
	Audit Keluar	Berhasil
	Audit Masuk	Sukses, Gagal
	Audit Peristiwa Masuk/Keluar Lainnya	Sukses, Gagal
	Audit Masuk Khusus	Sukses, Gagal

Kategori pemantauan	Pengaturan kebijakan	Status audit
Akses Objek	Audit Peristiwa Akses Objek Lainnya	Sukses, Gagal
	Audit Penyimpanan yang Dapat Dihapus	Sukses, Gagal
	Audit Pementasan Kebijakan Akses Pusat	Sukses, Gagal
Perubahan Kebijakan	Audit Perubahan Kebijakan	Sukses, Gagal
	Audit Perubahan Kebijakan Autentikasi	Sukses, Gagal
	Audit Perubahan Kebijakan Otorisasi	Sukses, Gagal
	Audit Perubahan Kebijakan Tingkat Aturan MPSSVC	Berhasil
	Audit Peristiwa Perubahan Kebijakan Lainnya	Kegagalan
Penggunaan Hak Istimewa	Audit Penggunaan Hak Istimewa Sensitif	Sukses, Gagal
Sistem	Audit Driver IPsec	Sukses, Gagal
	Audit Peristiwa Sistem Lainnya	Sukses, Gagal
	Audit Perubahan Status Keamanan	Sukses, Gagal
	Audit Ekstensi Sistem Keamanan	Sukses, Gagal
	Audit Integritas Sistem	Sukses, Gagal

Mengaktifkan penerusan log

Anda dapat menggunakan konsol AWS Directory Service atau API untuk meneruskan log peristiwa keamanan pengendali domain ke Amazon CloudWatch Logs. Hal ini membantu Anda untuk memenuhi persyaratan kebijakan pemantauan keamanan, audit, dan penyimpanan log Anda dengan menyediakan transparansi peristiwa keamanan di direktori Anda.

CloudWatch Logs juga dapat meneruskan peristiwa ini ke akun AWS lain, layanan AWS, atau aplikasi pihak ketiga. Hal ini memudahkan Anda untuk memantau dan mengonfigurasi peringatan secara terpusat untuk mendeteksi dan merespons secara proaktif aktivitas yang tidak biasa hampir secara real time.

Setelah diaktifkan, Anda dapat menggunakan konsol CloudWatch Logs untuk mengambil data dari grup log yang Anda tentukan saat mengaktifkan layanan. Grup log ini berisi log keamanan dari pengendali domain Anda.

Untuk informasi selengkapnya tentang grup log dan bagaimana cara membaca data mereka, lihat Bekerja dengan Grup Log dan Pengaliran Log di Panduan pengguna Amazon CloudWatch Logs.

> **Note**
>
> Penerusan log adalah fitur Regional dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk mengaktifkan penerusan log

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih ID direktori dari direktori Microsoft AD yang Dikelola AWS yang ingin Anda bagikan.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan penerusan log, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Penerusan log, pilih Aktifkan.

5. Pada dialog Mengaktifkan penerusan log ke CloudWatch, pilih salah satu opsi berikut:

    a. PilihMembuat grup log CloudWatch baru, di bawahNama grup CloudWatch Log, tentukan nama yang dapat Anda rujuk di CloudWatch Logs.

    b. Pilih Pilih grup log CloudWatch yang ada, dan di bawah Grup log CloudWatch yang ada, pilih grup log dari menu.

6. Tinjau informasi harga dan tautan, lalu pilih Aktifkan.

Untuk menonaktifkan penerusan log

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih ID direktori dari direktori Microsoft AD yang Dikelola AWS yang ingin Anda bagikan.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:

    - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menonaktifkan penerusan log, lalu pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
    - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.

4. Di bagian Penerusan log, pilih Nonaktifkan.
5. Setelah Anda membaca informasi di dialog Menonaktifkan penerusan log, pilih Nonaktifkan.

Menggunakan CLI untuk mengaktifkan penerusan log

Sebelum Anda dapat menggunakan perintah `ds create-log-subscription`, Anda harus terlebih dahulu membuat grup log Amazon CloudWatch, lalu membuat kebijakan sumber daya IAM yang akan memberikan izin yang diperlukan untuk grup tersebut. Untuk mengaktifkan penerusan log menggunakan CLI, selesaikan semua langkah di bawah ini.

Langkah 1: Membuat grup log di CloudWatch Logs

Membuat grup log yang akan digunakan untuk menerima log keamanan dari pengendali domain Anda. Kami merekomendasikan pra-pending nama dengan `/aws/directoryservice/`, tapi hal tersebut tidak diperlukan. Misalnya:

PERINTAH CONTOH CLI

```
aws logs create-log-group --log-group-name '/aws/directoryservice/
d-9876543210'
```

CONTOH PERINTAH POWERSHELL

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

Untuk petunjuk tentang cara membuat grup CloudWatch Logs, lihat Membuat grup log di CloudWatch Logs di Panduan Pengguna Amazon CloudWatch Logs.

Langkah 2: Membuat kebijakan sumber daya CloudWatch Logs di IAM

Membuat kebijakan sumber daya CloudWatch Logs yang memberikan hak AWS Directory Service untuk menambahkan log ke grup log baru yang Anda buat di Langkah 1. Anda dapat menentukan ARN yang tepat ke grup log untuk membatasiAWS Directory ServiceAkses ke grup log lain atau menggunakan wild card untuk menyertakan semua grup log. Contoh kebijakan berikut menggunakan metode wild card untuk mengidentifikasi bahwa semua grup log yang dimulai dengan `/aws/directoryservice/` untuk akun AWS di mana direktori anda berada akan disertakan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/*"
        }
    ]
}
```

Anda perlu menyimpan kebijakan ini ke file teks (misalnya Dspolicy.json) pada workstation lokal Anda karena Anda perlu menjalankannya dari CLI. Misalnya:

PERINTAH CONTOH CLI

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-
document file://DSPolicy.json
```

CONTOH PERINTAH POWERSHELL

```
$PolicyDocument = Get-Content .\DSPolicy.json –Raw

Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument
$PolicyDocument
```

Langkah 3: MembuatAWS Directory Servicelangganan log

Dalam langkah terakhir ini, Anda sekarang dapat melanjutkan untuk mengaktifkan penerusan log dengan membuat langganan log. Misalnya:

PERINTAH CONTOH CLI

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-
name '/aws/directoryservice/d-9876543210'
```

CONTOH PERINTAH POWERSHELL

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/
directoryservice/d-9876543210'
```

Pantau pengontrol domain Anda dengan metrik kinerja

AWS Directory Service terintegrasi dengan Amazon CloudWatch untuk membantu memberi Anda metrik kinerja penting untuk setiap pengontrol domain di Anda. Active Directory Ini berarti Anda dapat memantau penghitung kinerja pengontrol domain, seperti pemanfaatan CPU dan memori. Anda juga dapat mengonfigurasi alarm dan memulai tindakan otomatis untuk merespons periode pemanfaatan tinggi. Misalnya, Anda dapat mengonfigurasi alarm untuk pemanfaatan CPU pengontrol domain di atas 70 persen dan membuat topik SNS untuk memberi tahu Anda ketika ini terjadi. Anda dapat menggunakan topik SNS ini untuk memulai otomatisasi, seperti AWS Lambda fungsi, untuk meningkatkan jumlah pengontrol domain ke Anda. Active Directory

Untuk informasi selengkapnya tentang memantau pengontrol domain Anda, lihatTentukan kapan harus menambahkan pengontrol domain dengan metrik CloudWatch .

Ada biaya yang terkait dengan Amazon CloudWatch. Untuk informasi selengkapnya, lihat CloudWatchpenagihan dan biaya.

> **Important**
>
> Metrik kinerja pengontrol domain dengan tidak CloudWatch tersedia di Wilayah Kanada Barat (Calgary).

Temukan metrik kinerja pengontrol domain di CloudWatch

Di CloudWatch konsol Amazon, metrik untuk layanan tertentu dikelompokkan terlebih dahulu berdasarkan namespace layanan. Anda dapat menambahkan filter metrik yang berada di bawah namespace tersebut. Gunakan prosedur berikut untuk menemukan namespace dan metrik subordinat yang benar yang diperlukan untuk menyiapkan metrik pengontrol domain AWS Microsoft AD yang Dikelola. CloudWatch

Untuk menemukan metrik pengontrol domain di konsol CloudWatch

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, silakan pilih Metrik.
3. Dari daftar metrik, pilih namespace Directory Service, lalu dari daftar, pilih metrik AWS Microsoft AD yang dikelola.

Untuk petunjuk tentang cara mengatur metrik pengontrol domain menggunakan CloudWatch konsol, lihat Cara mengotomatiskan penskalaan AWS Microsoft AD Terkelola berdasarkan metrik pemanfaatan di Blog Keamanan. AWS

Tentukan kapan harus menambahkan pengontrol domain dengan metrik CloudWatch

Load balancing di semua pengontrol domain Anda penting untuk ketahanan dan kinerja Anda. Active Directory Untuk membantu mengoptimalkan kinerja pengontrol domain Anda di Microsoft AD yang AWS Dikelola, sebaiknya Anda memantau metrik penting terlebih dahulu CloudWatch untuk membentuk garis dasar. Selama proses ini, Anda menganalisis Active Directory dari waktu ke waktu untuk mengidentifikasi Active Directory pemanfaatan rata-rata dan puncak Anda. Setelah menentukan baseline Anda, Anda dapat memantau metrik ini secara teratur untuk membantu menentukan kapan harus menambahkan pengontrol domain ke Anda. Active Directory

Metrik berikut ini penting untuk dipantau secara teratur. Untuk daftar lengkap metrik pengontrol domain yang tersedia CloudWatch, lihatAWS Penghitung kinerja Microsoft AD yang dikelola.

- Metrik spesifik pengontrol domain, seperti:
  - Prosesor
  - Memori
  - Disk Logis
  - Antarmuka Jaringan
- AWS Metrik khusus direktori Microsoft AD yang dikelola, seperti:
  - Pencarian LDAP
  - Mengikat
  - Kueri DNS
  - Direktori dibaca
  - Direktori menulis

Untuk petunjuk tentang cara mengatur metrik pengontrol domain menggunakan CloudWatch konsol, lihat Cara mengotomatiskan penskalaan AWS Microsoft AD Terkelola berdasarkan metrik pemanfaatan di Blog Keamanan. AWS Untuk informasi umum tentang metrik di CloudWatch, lihat Menggunakan CloudWatch metrik Amazon di CloudWatch Panduan Pengguna Amazon.

Untuk informasi umum tentang perencanaan pengontrol domain, lihat Perencanaan kapasitas untuk Layanan Active Directory Domain di situs web Microsoft.

AWS Penghitung kinerja Microsoft AD yang dikelola

Tabel berikut mencantumkan semua penghitung kinerja yang tersedia di Amazon CloudWatch untuk melacak pengontrol domain dan kinerja direktori di Microsoft AD yang AWS Dikelola.

Kategori metrik	Nama metrik
Database ==> Contoh (NTDSA)	Database Cache% Hit
	Database I/O Membaca Latensi Rata-rata
	Bacaan Database I/O/detik
	I/O Log Menulis Latensi Rata-rata
DirectoryServices (NTDS)	Waktu Mengikat LDAP

Kategori metrik	Nama metrik
	Operasi Replikasi Tertunda DRA
	Sinkronisasi Replikasi Tertunda DRA
DNS	Pertanyaan rekursif/detik
	Kegagalan Kueri Rekursif/detik
	Kueri TCP Diterima/detik
	Total Kueri yang Diterima/detik
	Total Respon yang Dikirim/detik
	Kueri UDP Diterima/detik
LogicalDisk	Rata-rata. Panjang Antrean Cakram
	% Ruang Bebas
Memori	% Byte Berkomitmen dalam Penggunaan
	Seumur Hidup Cache Siaga Rata-Rata Jangka Panjang
Antarmuka Jaringan	Byte dikirim/detik
	Byte Diterima/detik
	Bandwidth saat ini
NTDS	ATQ Estimasi Penundaan Antrian
	Latensi Permintaan ATQ
	Direktori DS Membaca/Detik
	Pencarian Direktori DS/Detik
	Direktori DS Tulisan/Detik

Kategori metrik	Nama metrik
	Sesi Klien LDAP
	Pencarian LDAP/DETIK
	Ikatan Sukses LDAP/detik
Prosesor	% Waktu Prosesor
Statistik Seluruh Sistem Keamanan	Otentikasi Kerberos
	Otentikasi NTLM

Replikasi multi-Region

Replikasi Multi-Region dapat digunakan untuk secara otomatis mereplikasi data direktori AWS Microsoft AD Terkelola Anda di beberapa. Wilayah AWSReplikasi ini dapat meningkatkan kinerja bagi pengguna dan aplikasi di lokasi geografis yang tersebar. AWS Microsoft AD yang dikelola menggunakan replikasi Active Directory asli untuk mereplikasi data direktori Anda dengan aman ke Wilayah baru.

Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.

Anda dapat menggunakan replikasi Multi-wilayah otomatis di sebagian besar Wilayah tempat AWS Microsoft AD Terkelola tersedia.

Important

Replikasi Multi-Wilayah tidak tersedia di Wilayah keikutsertaan berikut:

- Africa (Cape Town) af-south-1
- Asia Pacific (Hong Kong) ap-east-1
- Asia Pasifik (Hyderabad) ap-selatan-2
- Asia Pasifik (Jakarta) ap-tenggara-3
- Asia Pasifik (Melbourne) ap-tenggara 4
- Kanada Barat (Calgary) ca-barat-1
- Eropa (Milan) eu-south-1

- Eropa (Spanyol) eu-selatan-2
- Eropa (Zurich) eu-central-2
- Israel (Tel Aviv) di pusat-1
- Middle East (Bahrain) me-south-1
- Timur Tengah (UEA) me-central-1

Untuk informasi selengkapnya tentang opt-in Regions dan cara mengaktifkannya, lihat Menentukan yang dapat digunakan akun Wilayah AWS Anda dalam AWS Account Management Panduan.

Manfaat

Dengan replikasi Multi-wilayah di AWS Microsoft AD yang Dikelola, aplikasi yang sadar Direktori Aktif menggunakan direktori secara lokal untuk kinerja tinggi dan fitur Multi-wilayah untuk ketahanan. Anda dapat menggunakan replikasi Multi-wilayah dengan aplikasi Active Directory-aware seperti SharePoint dan SQL Server Always On serta AWS layanan seperti Amazon RDS for SQL Server dan FSx for Windows File Server. Berikut ini adalah manfaat tambahan dari replikasi multi-Region.

- Ini memungkinkan Anda menerapkan satu instans Microsoft AD AWS Terkelola secara global, cepat, dan menghilangkan beban berat pengelolaan mandiri infrastruktur Direktori Aktif global.
- Ini membuatnya lebih mudah dan lebih hemat biaya bagi Anda untuk menyebarkan dan mengelola beban kerja Windows dan Linux di beberapa Wilayah. AWS Replikasi Multi-wilayah otomatis memungkinkan kinerja optimal dalam aplikasi sadar Direktori Aktif global Anda. Semua aplikasi yang digunakan di instans Windows atau Linux menggunakan AWS Microsoft AD yang Dikelola secara lokal di Wilayah, yang memungkinkan respons terhadap permintaan pengguna dari Wilayah terdekat.
- Ini memberikan ketahanan multi-Region. Diterapkan dalam infrastruktur AWS terkelola yang sangat tersedia, Microsoft AD yang AWS dikelola menangani pembaruan perangkat lunak otomatis, pemantauan, pemulihan, dan keamanan infrastruktur Direktori Aktif yang mendasarinya di semua Wilayah. Hal ini memungkinkan Anda untuk fokus membangun aplikasi Anda.

Topik

- Fitur Global vs Regional
- Region utama vs tambahan

- Cara kerja replikasi multi-Region
- Menambahkan Region yang direplikasi
- Menghapus Region yang direplikasi

Fitur Global vs Regional

Saat Anda menambahkan AWS Wilayah ke direktori Anda menggunakan replikasi Multi-wilayah, AWS Directory Service tingkatkan cakupan semua fitur sehingga menjadi sadar Wilayah. Fitur-fitur ini tercantum pada berbagai tab pada halaman detail yang muncul ketika Anda memilih ID dari direktori di konsol AWS Directory Service . Ini berarti bahwa semua fitur diaktifkan, dikonfigurasi, atau dikelola berdasarkan Region yang Anda pilih di bagian Replikasi multi-Region dari konsol tersebut. Perubahan yang Anda buat pada fitur di setiap Region diterapkan secara global atau per Region.

Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.

Fitur global

Setiap perubahan yang Anda buat untuk fitur global saat Region primer dipilih akan diterapkan di seluruh Region.

Anda dapat mengidentifikasi fitur yang digunakan secara global pada halaman Detail direktori karena mereka menampilkan Diterapkan untuk semua Region yang direplikasi di sampingnya. Atau, jika Anda memilih Region lain dalam daftar yang bukan Region primer, Anda dapat mengidentifikasi fitur yang digunakan secara global karena mereka menampilkan Diwarisi dari Region primer.

Fitur regional

Setiap perubahan yang Anda buat pada fitur di suatu fitur hanya Regional tambahan akan diterapkan ke Wilayah tersebut.

Anda dapat mengidentifikasi fitur yang digunakan secara global pada halaman Detail direktori karena mereka tidak menampilkan Diterapkan untuk semua Region yang direplikasi atau Diwarisi dari Region primer di sampingnya.

Region utama vs tambahan

Dengan replikasi Multi-wilayah, AWS Microsoft AD yang Dikelola menggunakan dua jenis Wilayah berikut untuk membedakan bagaimana fitur global atau Regional harus diterapkan di seluruh direktori Anda.

Region primer

Region awal tempat Anda pertama kali membuat direktori Anda disebut sebagai Region primer. Anda dapat melakukan operasi tingkat direktori global saja seperti membuat kepercayaan Active Directory dan memperbarui skema AD dari Region primer.

Region primer selalu dapat diidentifikasi sebagai Region pertama yang ditampilkan di bagian atas daftar di bagian Replikasi multi-Region, dan diakhiri dengan - Primer. Sebagai contoh, US East (N. Virginia) - Primer.

Setiap perubahan yang Anda buat untuk Fitur global saat Region primer dipilih akan diterapkan di seluruh Region.

Anda hanya dapat menambahkan Region saat Region primer dipilih. Untuk informasi selengkapnya, lihat Menambahkan Region yang direplikasi.

Regional tambahan

Setiap Daerah yang telah Anda tambahkan ke direktori Anda disebut sebagai Region Tambahan.

Meskipun beberapa fitur dapat dikelola secara global untuk semua Region, yang lainnya dikelola secara individual per Region. Untuk mengelola fitur untuk Region tambahan (Region non-primer), Anda harus terlebih dahulu memilih Region tambahan dari daftar di bagian Replikasi multi-Region pada halaman Detail direktori. Kemudian Anda dapat melanjutkan untuk mengelola fitur tersebut.

Setiap perubahan yang Anda buat untuk Fitur regional saat Region tambahan dipilih hanya akan diterapkan pada Region tersebut.

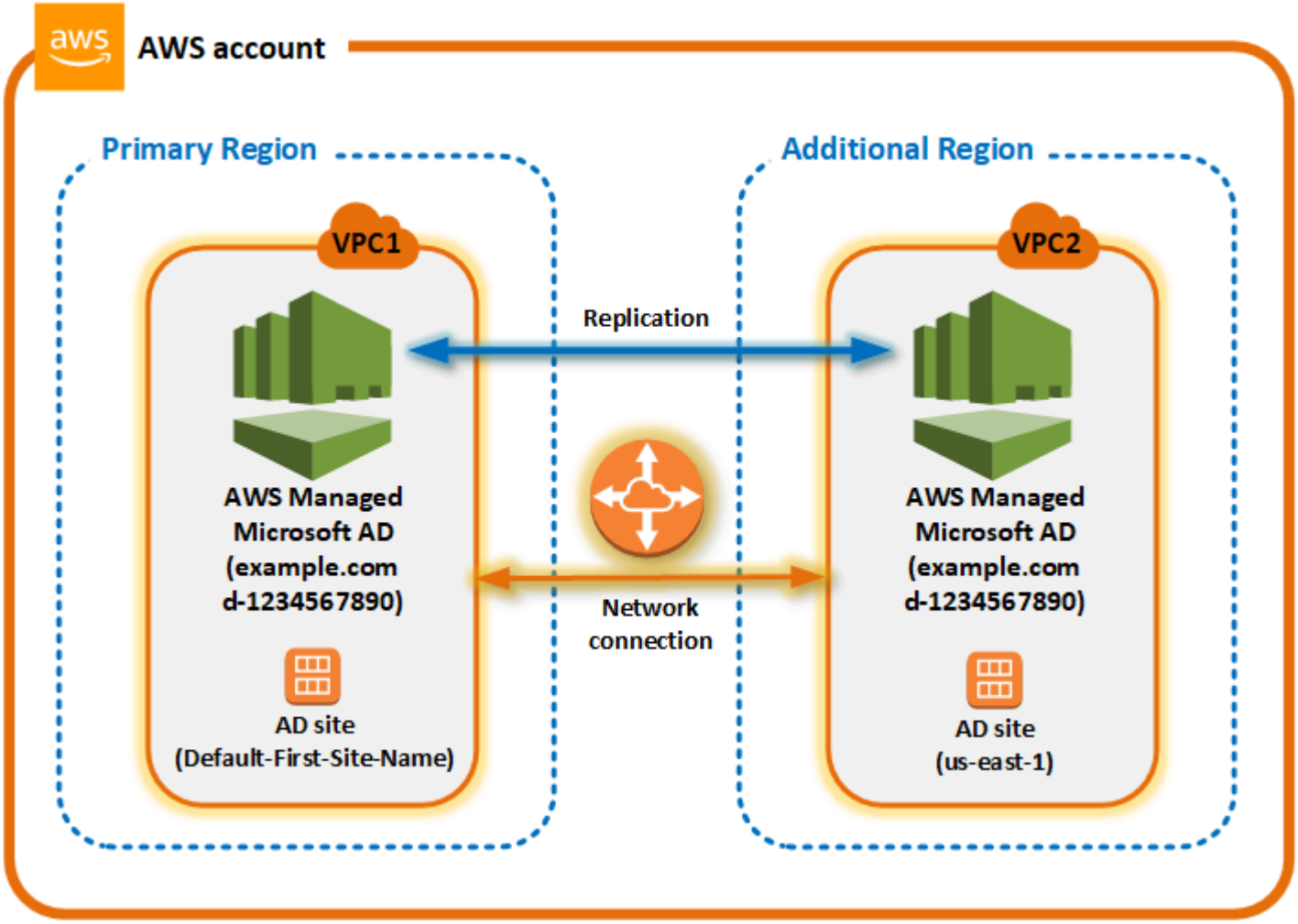
Cara kerja replikasi multi-Region

Dengan fitur replikasi Multi-wilayah, AWS Microsoft AD yang Dikelola menghilangkan beban berat yang tidak terdiferensiasi dalam mengelola infrastruktur Direktori Aktif global. Saat dikonfigurasi, AWS mereplikasi semua data direktori pelanggan termasuk pengguna, grup, kebijakan grup, dan skema di beberapa AWS Wilayah.

Setelah Region baru telah ditambahkan, operasi berikut secara otomatis terjadi seperti yang ditunjukkan dalam ilustrasi:

- AWS Microsoft AD yang dikelola membuat dua pengontrol domain di VPC yang dipilih dan menerapkannya ke Wilayah baru di akun yang sama. AWS Pengidentifikasi direktori Anda (`directory_id`) tetap sama di semua Region. Anda dapat menambahkan pengendali domain tambahan nanti jika Anda ingin.

- AWS Microsoft AD yang dikelola mengonfigurasi koneksi jaringan antara Wilayah utama dan Wilayah baru.
- AWS Microsoft AD yang dikelola membuat situs Direktori Aktif baru dan memberinya nama yang sama dengan Wilayah, seperti us-east-1. Anda juga dapat mengubah nama ini nanti menggunakan Situs dan Alat layanan Direktori Aktif.
- AWS Microsoft AD yang dikelola mereplikasi semua objek dan konfigurasi Direktori Aktif ke Wilayah baru, termasuk pengguna, grup, kebijakan grup, kepercayaan Direktori Aktif, unit organisasi, dan skema Direktori Aktif. Tautan situs Direktori Aktif dikonfigurasi untuk menggunakan Notifikasi Perubahan. Dengan perubahan notifikasi antara situs diaktifkan, perubahan menyebar ke situs jarak jauh dengan frekuensi yang sama yang mereka sebarkan dalam situs sumber, termasuk perubahan yang menjamin replikasi urgen.
- Jika ini adalah Wilayah pertama yang Anda tambahkan, Microsoft AD yang AWS Dikelola membuat semua fitur Multi-wilayah sadar. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.



Situs Direktori Aktif

Replikasi Multi-Region mendukung beberapa situs Direktori Aktif (satu situs Direktori Aktif per Wilayah). Ketika Region baru ditambahkan, itu diberi nama yang sama dengan Region tersebut —sebagai contoh, us-east-1. Anda juga dapat mengubah nama ini nanti menggunakan Situs dan Layanan Direktori Aktif.

AWS layanan

AWS layanan seperti Amazon RDS for SQL Server dan Amazon FSx terhubung ke instance lokal direktori global. Hal ini memungkinkan pengguna Anda untuk masuk sekali ke aplikasi Active Directory-aware yang berjalan serta AWS layanan seperti Amazon RDS for SQL Server di AWS Wilayah mana pun. AWS Untuk melakukannya, pengguna memerlukan kredensil dari AWS Microsoft AD yang Dikelola atau Direktori Aktif lokal jika Anda memiliki kepercayaan dengan iklan AWS Microsoft yang Dikelola.

Anda dapat menggunakan AWS layanan berikut dengan fitur replikasi Multi-wilayah.

- Amazon EC2
- FSx for Windows File Server
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

Pindah saat gagal/failover

Jika semua pengontrol domain di satu Wilayah sedang down, Microsoft AD yang AWS Dikelola memulihkan pengontrol domain dan mereplikasi data direktori secara otomatis. Sementara itu pengendali domain di Region lain tetap aktif dan berjalan.

Menambahkan Region yang direplikasi

Saat Anda menambahkan Wilayah menggunakan Replikasi multi-Region fitur tersebut, Microsoft AD yang AWS Dikelola akan membuat dua pengontrol domain di AWS Wilayah yang dipilih, Amazon

Virtual Private Cloud (VPC), dan subnet. AWS Microsoft AD yang dikelola juga membuat grup keamanan terkait yang memungkinkan beban kerja Windows terhubung ke direktori Anda di Wilayah baru. Ini juga menciptakan sumber daya ini menggunakan AWS akun yang sama di mana direktori Anda sudah digunakan. Anda melakukan ini dengan memilih Region, menentukan VPC, dan menyediakan konfigurasi untuk Region baru.

Replikasi Multi-Region hanya didukung untuk Edisi Perusahaan AWS Microsoft AD yang Dikelola.

Prasyarat

Sebelum melanjutkan langkah-langkah untuk menambahkan Region replikasi baru, kami rekomendasikan Anda terlebih dahulu meninjau tugas prasyarat berikut.

- Verifikasi bahwa Anda memiliki izin AWS Identity and Access Management (IAM) yang diperlukan, penyiapan Amazon VPC, dan pengaturan subnet di Wilayah baru tempat Anda ingin mereplikasi direktori.
- Jika Anda ingin menggunakan kredenal Direktori Aktif lokal yang ada untuk mengakses dan mengelola beban kerja yang sadar Direktori Aktif AWS, Anda harus membuat kepercayaan Direktori Aktif antara AWS Microsoft AD yang Dikelola dan infrastruktur AD lokal Anda. Untuk informasi selengkapnya tentang kepercayaan, lihat Connect ke infrastruktur Active Directory yang ada.
- Jika Anda memiliki hubungan kepercayaan yang ada antara Active Directory lokal dan ingin menambahkan wilayah yang direplikasi, Anda perlu memverifikasi bahwa Anda memiliki pengaturan VPC dan subnet Amazon yang diperlukan di Wilayah baru tempat Anda ingin mereplikasi direktori.

Tambahkan Region.

Gunakan prosedur berikut untuk menambahkan Wilayah yang direplikasi untuk direktori Microsoft AD AWS Terkelola Anda.

Untuk menambahkan Region yang direplikasi

1. Pada panel navigasi konsolAWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, di bawah Replikasi multi-Region, pilih Region Primer dari daftar, dan kemudian pilih Tambahkan Region.

> **Note**
>
> Anda hanya dapat menambahkan Region saat Region Primer dipilih. Untuk informasi selengkapnya, lihat Region primer.

4. Pada halaman Tambahkan Region, di bawah Region, pilih Region yang ingin Anda tambahkan dari daftar.
5. Di bawah VPC, pilih VPC yang akan digunakan untuk Region ini.

> **Note**
>
> VPC ini tidak boleh memiliki Classless Inter-Domain Routing (CIDR) yang tumpang tindih dengan VPC yang digunakan oleh direktori ini di Region lain.

6. Di bawah Subnet, pilih subnet yang akan digunakan untuk Region ini.
7. Tinjau informasi di bawah Harga, lalu pilih Tambahkan.
8. Saat Microsoft AD yang AWS Dikelola menyelesaikan proses penyebaran pengontrol domain, Wilayah akan menampilkan status Aktif. Sekarang Anda dapat melakukan pembaruan ke Wilayah ini sesuai kebutuhan.

Langkah selanjutnya

Setelah menambahkan Region baru, Anda harus pertimbangkan untuk melakukan langkah-langkah berikut:

- Men-deploy pengendali domain tambahan (hingga 20) ke Region baru Anda sesuai kebutuhan. Jumlah pengendali domain ketika Anda menambahkan Region baru adalah 2 secara default, yang merupakan minimum yang diperlukan untuk toleransi kesalahan dan tujuan ketersediaan tinggi. Untuk informasi selengkapnya, lihat Menambah atau menghapus pengendali domain tambahan.
- Bagikan direktori Anda dengan lebih banyak AWS akun per Wilayah. Konfigurasi berbagi direktori tidak direplikasi dari Region primer secara otomatis. Untuk informasi selengkapnya, lihat Bagikan direktori Anda.
- Aktifkan penerusan log untuk mengambil log keamanan direktori Anda menggunakan CloudWatch Log Amazon dari Wilayah baru. Saat Anda mengaktifkan penerusan log, Anda harus memberikan nama grup log di setiap Region di mana Anda mereplikasikan direktori Anda. Untuk informasi selengkapnya, lihat Mengaktifkan penerusan log.

- Aktifkan pemantauan Amazon Simple Notification Service (Amazon SNS) untuk Region baru untuk melacak status kondisi direktori Anda per Wilayah. Untuk informasi selengkapnya, lihat Konfigurasikan pemberitahuan status direktori dengan Amazon SNS.

Menghapus Region yang direplikasi

Gunakan prosedur berikut untuk menghapus Wilayah untuk direktori Microsoft AD yang AWS Dikelola. Sebelum Anda menghapus Region, pastikan tidak memiliki salah satu dari berikut ini:

- Aplikasi otorisasi yang melekat padanya.
- Direktori bersama yang terkait dengannya.

Untuk menghapus Region yang direplikasi

1. Pada panel navigasi konsolAWS Directory Service, pilih Direktori.
2. Dari bilah navigasi, pilih pemilih Wilayah dan pilih wilayah tempat direktori Anda disimpan.
3. Pada halaman Direktori, pilih ID direktori Anda.
4. Pada halaman Detail direktori, di bawah Replikasi multi-Region pilih Hapus Region.
5. Di kotak dialog Hapus Region, tinjau informasi, dan kemudian masukkan dalam nama wilayah untuk mengkonfirmasi. Lalu pilih Hapus.

> **Note**
>
> Anda tidak dapat membuat pembaruan ke Region saat sedang dihapus.

Bagikan direktori Anda

Microsoft AD yang Dikelola AWS terintegrasi erat dengan AWS Organizations untuk memungkinkan berbagi direktori secara mulus di beberapa akun AWS. Anda dapat berbagi direktori tunggal dengan akun AWS terpercaya lainnya dalam organisasi yang sama atau berbagi direktori dengan akun AWS yang berada di luar organisasi Anda. Anda juga dapat berbagi direktori Anda saat akun AWS saat ini bukan anggota organisasi.

> **Note**
>
> AWS mengenakan biaya tambahan untuk berbagi direktori. Untuk mempelajari selengkapnya, lihat halaman Harga di situs web Directory Service AWS.

Berbagi direktori membuat Microsoft AD yang Dikelola AWS lebih hemat biaya untuk mengintegrasikan dengan Amazon EC2 di beberapa akun dan VPC. Berbagi direktori tersedia di semua Region AWS di mana Microsoft AD yang dikelola AWS ditawarkan.

> **Note**
>
> Di Region China (Ningxia) AWS , fitur ini hanya tersedia saat menggunakan AWSSystems Manager (SSM) untuk menggabungkan instans Amazon EC2 Anda secara mulus.

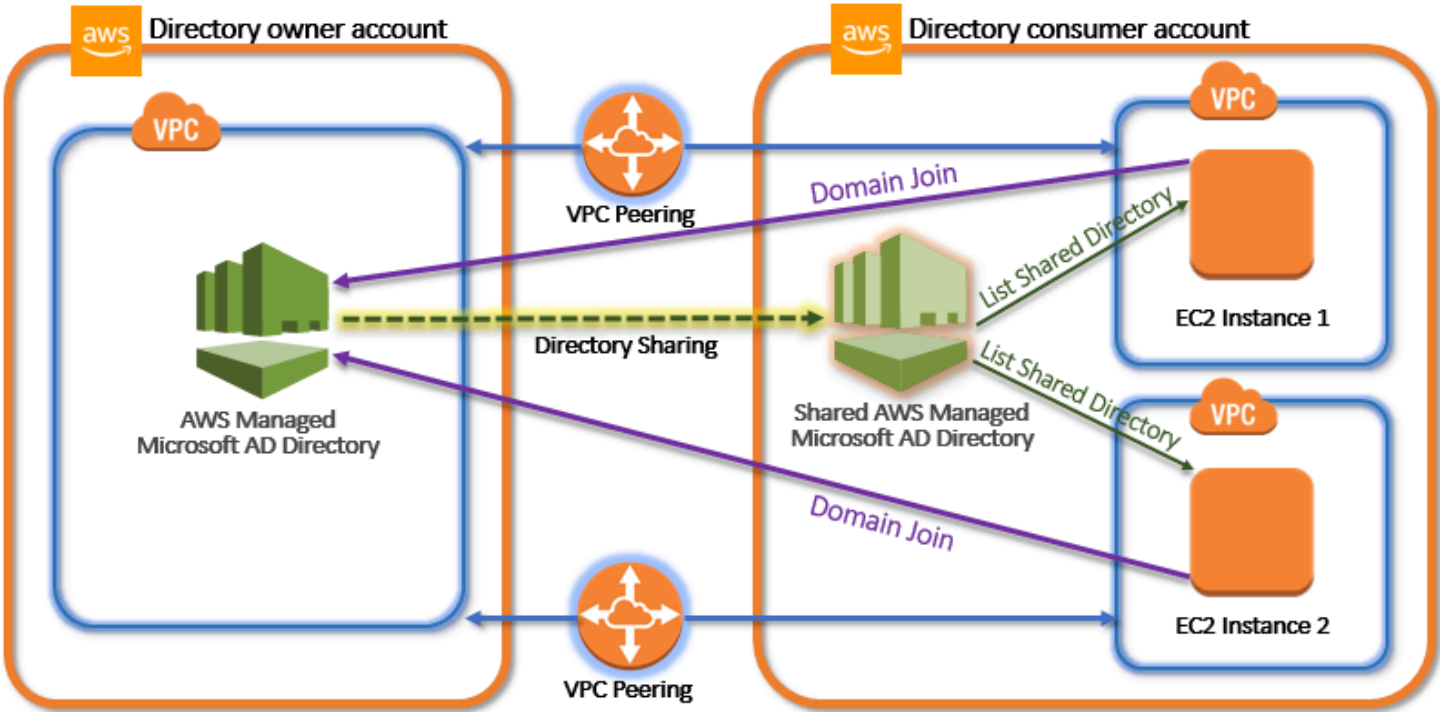
Untuk informasi lebih lanjut tentang berbagi direktori dan cara memperluas jangkauan dari direktori Microsoft AD yang Dikelola AWS Anda di batas akun AWS, lihat topik berikut.

Topik

- Konsep berbagi direktori kunci
- Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus
- Batalkan berbagi direktori Anda

Konsep berbagi direktori kunci

Anda akan mendapatkan lebih banyak fitur berbagi direktori jika Anda terbiasa dengan konsep-konsep kunci berikut.



Akun pemilik direktori

Pemilik direktori adalah pemegang Akun AWS yang memiliki direktori asal dalam hubungan direktori bersama. Administrator di akun ini memulai alur kerja berbagi direktori dengan menentukan Akun AWS mana yang akan dibagikan direktorinya. Pemilik direktori dapat melihat siapa yang telah mereka bagikan direktori dengan menggunakan tab Skala & Bagikan untuk direktori yang diberikan dalam konsol AWS Directory Service.

Akun konsumen direktori

Dalam hubungan direktori bersama, konsumen direktori mewakili Akun AWS yang di mana pemilik direktori berbagi direktori. Tergantung pada metode berbagi yang digunakan, administrator di akun ini mungkin perlu menerima undangan yang dikirim dari pemilik direktori sebelum mereka dapat mulai menggunakan direktori bersama.

Proses berbagi direktori membuat direktori bersama di akun konsumen direktori. Direktori bersama ini berisi metadata yang memungkinkan instans EC2 untuk menggabungkan domain secara mulus, yang menempatkan direktori asal di akun pemilik direktori. Setiap direktori bersama dalam akun konsumen direktori memiliki pengenal unik (ID direktori bersama).

Metode berbagi

Microsoft AD yang Dikelola AWS menyediakan dua metode berbagi direktori berikut:

- AWS Organizations – Metode ini memudahkan untuk berbagi direktori dalam organisasi Anda karena Anda dapat menelusuri dan memvalidasi akun konsumen direktori. Untuk menggunakan opsi ini, organisasi Anda harus memiliki Semua fitur, dan direktori Anda harus berada dalam akun pengelolaan organisasi. Metode berbagi ini menyederhanakan pengaturan Anda karena tidak memerlukan akun konsumen direktori untuk menerima permintaan berbagi direktori Anda. Di konsol tersebut, metode ini disebut sebagai Bagikan direktori ini dengan Akun AWS di dalam organisasi Anda.
- Jabat Tangan – Metode ini memungkinkan berbagi direktori ketika Anda tidak menggunakan AWS Organizations. Metode jabat tangan memerlukan akun konsumen direktori untuk menerima permintaan berbagi direktori. Di konsol tersebut, metode ini disebut sebagai Bagikan direktori ini dengan Akun AWS lain.

Konektivitas jaringan

Konektivitas jaringan merupakan prasyarat untuk menggunakan berbagi direktori di Akun AWS. AWS mendukung banyak solusi untuk menghubungkan VPC Anda, beberapa di antaranya termasuk Peering VPC, Transit Gateway, dan VPN. Untuk memulai, lihat Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus.

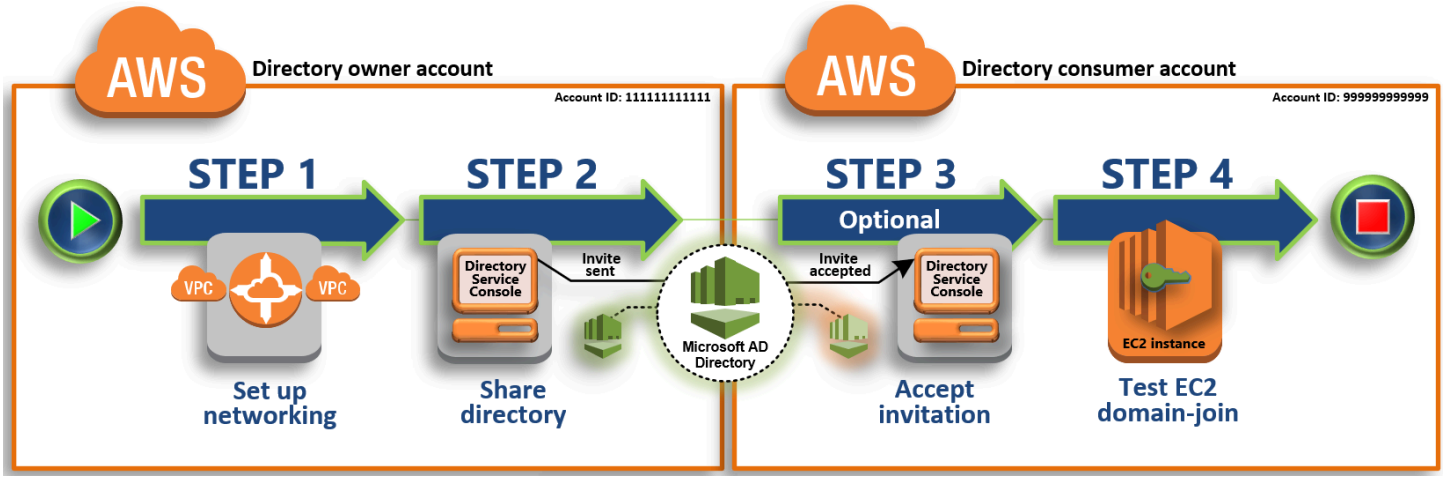
Tutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus

Tutorial ini menunjukkan cara berbagi direktori Microsoft AD AWS Terkelola Anda (akun pemilik direktori) dengan yang lain Akun AWS (akun konsumen direktori). Setelah prasyarat jaringan selesai, Anda akan berbagi direktori antara dua. Akun AWS Kemudian Anda akan belajar cara menggabungkan instans EC2 secara mulus ke domain di akun konsumen direktori.

Kami merekomendasikan Anda untuk terlebih dahulu meninjau konsep kunci berbagi direktori dan menggunakan konten kasus sebelum Anda mulai bekerja pada tutorial ini. Untuk informasi selengkapnya, lihat Konsep berbagi direktori kunci.

Proses untuk berbagi direktori berbeda tergantung pada apakah Anda berbagi direktori dengan yang lain Akun AWS di AWS organisasi yang sama atau dengan akun yang berada di luar AWS organisasi. Untuk informasi selengkapnya tentang cara berbagi, lihat Metode berbagi.

Alur kerja ini memiliki empat langkah dasar.



[Langkah 1: Atur lingkungan jaringan Anda]

Di akun pemilik direktori, Anda mengatur semua prasyarat jaringan yang diperlukan untuk proses berbagi direktori.

[Langkah 2: Bagikan direktori Anda]

Saat masuk dengan kredensial administrator pemilik direktori, Anda membuka konsol AWS Directory Service dan memulai alur kerja berbagi direktori, yang mengirimkan undangan ke akun konsumen direktori.

[Langkah 3: Terima undangan direktori bersama - Opsional]

Saat masuk dengan kredensi administrator konsumen direktori, Anda membuka AWS Directory Service konsol dan menerima undangan berbagi direktori.

[Langkah 4: Uji menggabungkan instans EC2 secara mulus untuk Windows Server ke domain]

Akhirnya, sebagai administrator direktori konsumen, Anda mencoba untuk menggabungkan instans EC2 untuk domain Anda dan memverifikasi bahwa itu bekerja.

Sumber daya tambahan

- [Kasus penggunaan: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 dengan mulus ke domain di seluruh Akun AWS]
- [AWS Artikel Blog Keamanan: Cara Menggabungkan Instans Amazon EC2 Dari Beberapa Akun dan VPC ke Satu Direktori Microsoft AD yang Dikelola AWS]

Langkah 1: Atur lingkungan jaringan Anda

Sebelum Anda mulai langkah-langkah dalam tutorial ini, Anda harus terlebih dahulu melakukan hal berikut ini:

- Buat dua yang baru Akun AWS untuk tujuan pengujian di Wilayah yang sama. Saat Anda membuat Akun AWS, secara otomatis membuat cloud pribadi virtual (VPC) khusus di setiap akun. Perhatikan ID VPC di setiap akun. Anda akan membutuhkan ini nanti.
- Buat koneksi peering VPC antara kedua VPC di setiap akun menggunakan prosedur dalam langkah ini.

> **Note**
>
> Meskipun ada banyak cara untuk menghubungkan pemilik direktori dan VPC akun konsumen Direktori, tutorial ini akan menggunakan metode peering VPC. Untuk opsi konektivitas VPC tambahan, lihat Konektivitas jaringan.

Mengkonfigurasi koneksi peering VPC antara pemilik direktori dan akun konsumen direktori

Koneksi peering VPC yang akan Anda buat adalah antara direktori konsumen dan VPC pemilik direktori. Ikuti langkah-langkah berikut untuk mengkonfigurasi koneksi peering VPC untuk konektivitas dengan akun konsumen direktori. Dengan koneksi ini Anda dapat merutekan lalu lintas antara kedua VPC menggunakan alamat IP privat.

Untuk membuat koneksi peering VPC antara pemilik direktori dan akun konsumen direktori

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/. Pastikan untuk masuk sebagai pengguna dengan kredensial administrator di akun pemilik direktori.
2. Di panel navigasi, pilih Koneksi Peering. Lalu pilih Buat Koneksi Peering.
3. Konfigurasi informasi berikut:
   - Label nama koneksi peering: Menyediakan nama yang jelas mengidentifikasi hubungan ini dengan VPC di akun konsumen direktori.
   - VPC (Peminta): Pilih ID VPC untuk akun pemilik direktori.
   - Di bawah Pilih VPC lain untuk di-peer, pastikan bahwa Akun saya dan Region ini dipilih.
   - VPC (Penerima): Pilih ID VPC untuk akun konsumen direktori.
4. Pilih Buat Koneksi Peering. Di kotak dialog konfirmasi, pilih OK.

Karena kedua VPC berada di Region yang sama, administrator dari akun pemilik direktori yang mengirim permintaan peering VPC juga dapat menerima permintaan peering atas nama akun konsumen direktori.

Untuk menerima permintaan peering atas nama akun konsumen direktori

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Koneksi Peering.
3. Pilih koneksi peering VPC yang tertunda. (Statusnya adalah Penerimaan Tertunda.) Pilih Tindakan, Terima Permintaan.
4. Dalam dialog konfirmasi, pilih Ya, Terima. Di kotak dialog konfirmasi berikutnya, pilih Modifikasi tabel rute saya sekarang untuk pergi langsung ke halaman tabel rute.

Sekarang koneksi peering VPC Anda aktif, Anda harus menambahkan entri ke tabel rute VPC Anda di akun pemilik direktori. Melakukan hal ini memungkinkan lalu lintas untuk diarahkan ke VPC dalam akun direktori konsumen.

Untuk menambahkan entri ke tabel rute VPC di akun pemilik direktori

1. Saat di bagian Tabel rute dari konsol Amazon VPC, pilih tabel rute untuk VPC pemilik direktori.
2. Pilih tab Rute, pilih Edit rute, dan kemudian pilih Tambahkan rute.
3. Di kolom Tujuan, masukkan blok CIDR untuk VPC konsumen direktori.
4. Di kolom Target, masukkan ID koneksi peering VPC (seperti**`pcx-123456789abcde000`**) untuk koneksi peering yang Anda buat sebelumnya di akun pemilik direktori.
5. Pilih Simpan perubahan.

Untuk menambahkan entri ke tabel rute VPC di akun konsumen direktori

1. Saat di bagian Tabel rute dari konsol Amazon VPC, pilih tabel rute untuk VPC konsumen direktori.
2. Pilih tab Rute, pilih Edit rute, dan kemudian pilih Tambahkan rute.
3. Di kolom Tujuan, masukkan blok CIDR untuk VPC pemilik direktori.
4. Di kolom Target, ketik ID koneksi peering VPC (seperti**`pcx-123456789abcde001`**) untuk koneksi peering yang Anda buat sebelumnya di akun konsumen direktori.
5. Pilih Simpan perubahan.

Pastikan untuk mengkonfigurasi grup keamanan VPC konsumen direktori Anda untuk mengaktifkan lalu lintas keluar dengan menambahkan protokol Direktori Aktif dan port-port ke tabel aturan keluar. Untuk informasi selengkapnya, lihat Grup keamanan untuk VPC Anda dan AWS Prasyarat Microsoft AD yang terkelola.

Langkah Selanjutnya

Langkah 2: Bagikan direktori Anda

Langkah 2: Bagikan direktori Anda

Gunakan prosedur berikut untuk memulai alur kerja berbagi direktori dari dalam akun pemilik direktori.

> **Note**
>
> Berbagi direktori adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk berbagi direktori Anda dari akun pemilik direktori

1. Masuk ke kredensi administrator AWS Management Console with di akun pemilik direktori dan buka AWS Directory Service konsol di https://console.aws.amazon.com/directoryservicev2/.
2. Di panel navigasi, pilih Direktori.
3. Pilih ID direktori direktori Microsoft AD AWS Terkelola yang ingin Anda bagikan.
4. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin membagikan direktori Anda, lalu pilih tab Menskalakan & bagikan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Menskalakan & bagikan.
5. Di bagian Direktori bersama, pilih Tindakan, lalu pilih Buat direktori bersama baru.
6. Pada halaman Pilih mana Akun AWS yang akan dibagikan, pilih salah satu metode berbagi berikut tergantung pada kebutuhan bisnis Anda:

a. Bagikan direktori ini dengan Akun AWS di dalam organisasi Anda — Dengan opsi ini Akun AWS Anda dapat memilih direktori yang ingin Anda bagikan dari daftar yang menunjukkan semua bagian Akun AWS dalam AWS organisasi Anda. Anda harus mengaktifkan akses tepercaya dengan AWS Directory Service sebelum Anda berbagi direktori. Untuk informasi selengkapnya, lihat Cara mengaktifkan atau menonaktifkan akses tepercaya.

> **Note**
>
> Untuk menggunakan opsi ini, organisasi Anda harus memiliki Semua fitur, dan direktori Anda harus berada dalam akun pengelolaan organisasi.

   i. Akun AWS Di bawah di organisasi Anda, pilih direktori Akun AWS yang ingin Anda bagikan dan klik Tambah.

   ii. Tinjau detail harga, lalu pilih Bagikan.

   iii. Lanjutkan ke Langkah 4 dalam panduan ini. Karena semua Akun AWS berada di organisasi yang sama, Anda tidak perlu mengikuti Langkah 3.

b. Bagikan direktori ini dengan yang lain Akun AWS - Dengan opsi ini, Anda dapat berbagi direktori dengan akun di dalam atau di luar AWS organisasi Anda. Anda juga dapat menggunakan opsi ini ketika direktori Anda bukan anggota AWS organisasi dan Anda ingin berbagi dengan yang lain Akun AWS.

   i. Di ID Akun AWS , masukkan semua ID Akun AWS yang Anda ingin berbagi direktori, dan kemudian klik Tambahkan.

   ii. Di Kirim catatan, ketik pesan ke administrator di Akun AWS lain.

   iii. Tinjau detail harga, lalu pilih Bagikan.

   iv. Lanjutkan ke Langkah 3.

Langkah Selanjutnya

Langkah 3: Terima undangan direktori bersama - Opsional

Langkah 3: Terima undangan direktori bersama - Opsional

Jika Anda memilih Bagikan direktori ini dengan Akun AWS (metode jabat tangan) pilihan dalam prosedur sebelumnya, Anda harus menggunakan prosedur ini untuk menyelesaikan alur kerja

direktori bersama. Jika Anda memilih opsi Bagikan direktori ini dengan Akun AWS di dalam organisasi Anda, lewati langkah ini dan lanjutkan ke Langkah 4.

Untuk menerima undangan direktori bersama

1. Masuk ke kredensi administrator AWS Management Console dengan di akun konsumen direktori dan buka AWS Directory Service konsol di https://console.aws.amazon.com/directoryservicev2/.
2. Di panel navigasi, pilih Direktori yang dibagikan dengan saya.
3. Di kolom ID Direktori bersama, pilih ID direktori yang ada dalam keadaan Penerimaan tertunda.
4. Pada halaman Detail direktori bersama, pilih Tinjauan.
5. Di dialog Undangan direktori bersama tertunda, tinjau catatan, detail pemilik direktori, dan informasi tentang harga. Jika Anda setuju, pilih Terima untuk mulai menggunakan direktori.

Langkah Selanjutnya

Langkah 4: Uji menggabungkan instans EC2 secara mulus untuk Windows Server ke domain

Langkah 4: Uji menggabungkan instans EC2 secara mulus untuk Windows Server ke domain

Anda dapat menggunakan salah satu dari dua metode berikut untuk menguji dengan mulus menggabungkan instans EC2 ke domain.

Metode 1: Menguji penggabungan domain menggunakan konsol Amazon EC2

Gunakan langkah-langkah ini di direktori akun konsumen.

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).

7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.

   a. Untuk membuat key pair baru, pilih Create new key pair.

   b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.

   c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.

   d. Pilih create key pair.

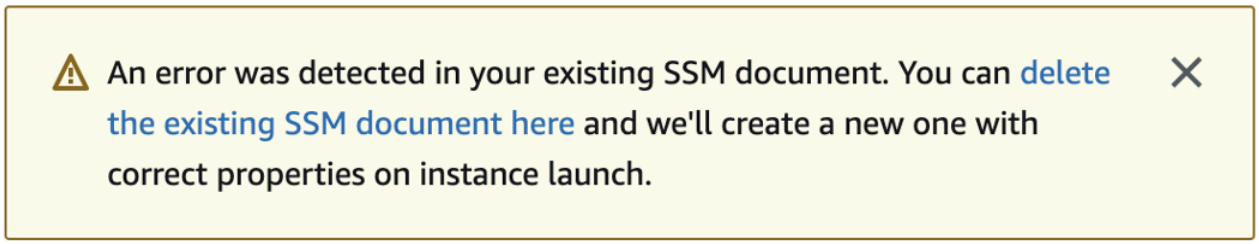
   e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

   > **Important**
   >
   > Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

    Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:
>
> 
>
>
> Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:
>
> - Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
> - Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola AmazonSSM ManagedInstanceCore dan AmazonSSM yang DirectoryServiceAccess dilampirkan padanya dari daftar tarik-turun profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

    1. Pilih Buat peran.
    2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.
    3. Di bawah Kasus penggunaan, pilih EC2.
    4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih kebijakan AmazonSSM dan AmazonSSM ManagedInstanceCore. DirectoryServiceAccess Untuk memfilter daftar, **`SSM`** ketik kotak pencarian. Pilih Berikutnya.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk

menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
7. Pilih Buat peran.
8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.

16. Pilih Luncurkan instans.

Metode 2: Uji domain bergabung menggunakan AWS Systems Manager

Gunakan langkah-langkah ini di direktori akun konsumen. Untuk menyelesaikan prosedur ini, Anda memerlukan beberapa informasi tentang akun pemilik direktori seperti ID Direktori, nama direktori, dan alamat IP DNS.

Prasyarat

- Pengaturan AWS Systems Manager.
  - Untuk informasi selengkapnya tentang Systems Manager, lihat Penyiapan umum untuk AWS Systems Manager.
- Instans yang ingin Anda gabungkan dengan domain Direktori Aktif Microsoft AWS Terkelola harus memiliki peran IAM terlampir yang berisi kebijakan terkelola AmazonSSM dan AmazonSSM ManagedInstanceCore. DirectoryServiceAccess
  - Untuk informasi selengkapnya tentang kebijakan terkelola ini dan kebijakan lain yang dapat Anda lampirkan ke profil instans IAM untuk Systems Manager, lihat Membuat profil instans IAM untuk Systems Manager di AWS Systems Manager Panduan Pengguna. Untuk informasi selengkapnya tentang kebijakan terkelola , lihat Kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang penggunaan Systems Manager untuk menggabungkan instans EC2 ke domain Direktori Aktif AWS Microsoft Terkelola, lihat Bagaimana cara menggunakan

AWS Systems Manager instans Windows EC2 yang sedang berjalan ke domain AWS Directory Service saya? .

1. Buka AWS Systems Manager konsol dihttps://console.aws.amazon.com/systems-manager/.
2. Di panel navigasi, di bawah Manajemen Node, pilih Jalankan Perintah.
3. Pilih Run command.
4. Pada halaman Run command, cari `AWS-JoinDirectoryServiceDomain`. Ketika ditampilkan dalam hasil pencarian, pilih pilihan `AWS-JoinDirectoryServiceDomain`.
5. Scroll ke bawah ke bagian Parameter perintah. Anda harus memberikan parameter berikut:

   > **Note**
   >
   > Anda dapat menemukan ID Direktori, nama direktori, dan alamat IP DNS dengan kembali ke AWS Directory Service konsol, memilih Direktori yang dibagikan dengan saya, dan memilih direktori Anda. ID Direktori Anda dapat ditemukan di bagian Detail direktori bersama. Anda dapat menemukan nilai untuk nama Direktori dan alamat IP DNS di bawah bagian detail direktori Pemilik.

   - Untuk ID Direktori, masukkan nama Direktori Aktif Microsoft yang AWS Dikelola.
   - Untuk Nama Direktori, masukkan nama Direktori Aktif Microsoft AWS Terkelola (untuk akun pemilik direktori).
   - Untuk Alamat IP DNS, masukkan alamat IP server DNS di Direktori Aktif AWS Microsoft Terkelola (untuk akun pemilik direktori).
6. Untuk Target, pilih Pilih instance secara manual, lalu pilih instance yang ingin Anda gabungkan dengan domain.
7. Biarkan sisa formulir diatur ke nilai default mereka, scroll ke bawah halaman, dan kemudian pilih Jalankan.
8. Status perintah akan berubah dari Pending menjadi Success setelah instance berhasil bergabung dengan domain. Anda dapat melihat output perintah dengan memilih ID Instance dari instance yang bergabung dengan domain dan View output.

Setelah menyelesaikan salah satu dari langkah-langkah ini, Anda sekarang dapat menggabungkan instans EC2 Anda ke domain. Setelah melakukannya, Anda dapat masuk ke instans menggunakan

klien Remote Desktop Protocol (RDP) dengan kredensil dari akun pengguna AWS Microsoft AD yang Dikelola.

Batalkan berbagi direktori Anda

Gunakan prosedur berikut untuk membatalkan berbagi direktori Microsoft AD yang Dikelola AWS.

Untuk membatalkan berbagi direktori Anda

1. Di panel navigasi Konsol AWS Directory Service, di bawah Direktori Aktif, pilih Direktori.
2. Pilih ID direktori dari direktori Microsoft AD yang Dikelola AWS yang ingin Anda batalkan berbagi.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Daerah yang ditampilkan di bawah Replikasi multi-Region, pilih Region tempat Anda ingin membatalkan berbagi direktori Anda, lalu pilih tab Menskalakan & bagikan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Menskalakan & bagikan.
4. Di Direktori bersama, pilih direktori bersama yang ingin Anda batalkan berbagi, pilih Tindakan, lalu pilih Batalkan Berbagi.
5. Di kotak dialog Batalkan berbagi direktori, pilih Batalkan Berbagi.

Sumber daya tambahan

- Kasus penggunaan: Bagikan direktori Anda untuk menggabungkan instans Amazon EC2 secara mulus ke seluruh domainAWSrekening
- AWSartikel blog keamanan: Cara untuk menggabungkan instans Amazon EC2 dari beberapa akun dan VPC untuk satuAWSDirektori Microsoft AD yang Dikelola
- Menggabungkan instans DB Amazon RDS Anda di seluruh akun ke domain bersama tunggal

Bergabunglah dengan instans Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola

Anda dapat menggabungkan instans Amazon EC2 dengan mulus ke domain Active Directory Anda saat instans diluncurkan. Untuk informasi selengkapnya, lihat Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory. Anda juga dapat

meluncurkan instans EC2 dan menggabungkannya ke Active Directory domain langsung dari AWS Directory Service konsol dengan AWS Systems Manager Automation.

Jika Anda perlu menggabungkan instans EC2 secara manual ke Active Directory domain Anda, Anda harus meluncurkan instance di Wilayah dan grup keamanan atau subnet yang tepat, lalu bergabung dengan instance tersebut ke domain.

Untuk dapat terhubung dari jarak jauh ke instans ini, Anda harus memiliki konektivitas IP ke instans dari jaringan di mana Anda menghubungkannya dari. Dalam kebanyakan kasus, ini mengharuskan gateway internet dilampirkan ke VPC Anda dan instans tersebut memiliki alamat IP publik.

Topik

- Luncurkan instans administrasi direktori di Microsoft AD AWS Terkelola Active Directory
- Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory
- Menggabungkan instans Windows Amazon EC2 secara manual ke Direktori Aktif AWS Microsoft AD Terkelola
- Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AWS AD Terkelola
- Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola
- Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola menggunakan Winbind
- Menggabungkan instans Amazon EC2 Mac secara manual ke Direktori Aktif AWS Microsoft AD Terkelola
- Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS
- Buat set opsi DHCP

Luncurkan instans administrasi direktori di Microsoft AD AWS Terkelola Active Directory

Prosedur ini meluncurkan administrasi direktori EC2 Windows instans dalam AWS Management Console menggunakan AWS Systems Manager Automation untuk mengelola direktori Anda. Anda juga dapat melakukannya dengan menjalankan otomatisasi AWS-Createds ManagementInstance di konsol Otomasi secara langsung. AWS Systems Manager

Prasyarat

Untuk meluncurkan instans EC2 administrasi direktori dari konsol, Anda harus mengaktifkan izin berikut di akun Anda.

- `ds:DescribeDirectories`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2:DeleteSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:DeleteInstanceProfile`
- `iam:DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfiles`
- `iam:ListInstanceProfilesForRole`
- `iam:PassRole`

- `iam:RemoveRoleFromInstanceProfile`
- `iam:TagInstanceProfile`
- `iam:TagRole`
- `ssm:CreateDocument`
- `ssm:DeleteDocument`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `ssm:GetDocument`

Untuk meluncurkan instans EC2 administrasi direktori di AWS Management Console

1. Masuk ke konsol AWS Directory Service tersebut.
2. Di bawah Active Directory, pilih Direktori.
3. Pilih ID Direktori direktori tempat Anda ingin meluncurkan instans EC2 administrasi Active Directory.
4. Pada halaman direktori, di pojok kanan atas, pilih Tindakan.
5. Di dropdown Actions, pilih Launch directory administration EC2 instance.
6. Pada halaman instans EC2 administrasi direktori Launch, di bawah parameter Input, lengkapi bidangnya.
7. (Opsional) Pilih Lihat AWS CLI perintah untuk melihat contoh yang Anda gunakan AWS CLI untuk menjalankan otomatisasi ini.
8. Pilih Kirim.
9. Anda dibawa kembali ke halaman direktori. Flashbar hijau ditampilkan di bagian atas layar Anda untuk menunjukkan bahwa Anda berhasil memulai peluncuran.

Untuk melihat administrasi direktori EC2 instans

Jika Anda belum meluncurkan instans EC2 apa pun untuk direktori, tanda hubung (-) ditampilkan di bawah instans EC2 administrasi direktori.

1. Di bawah Active Directory, pilih Direktori dan pilih direktori yang ingin Anda lihat.
2. Di bawah Detail direktori, di bawah Instans EC2 administrasi direktori, pilih satu atau semua instance Anda untuk dilihat.
3. Saat memilih instans, Anda diarahkan ke halaman EC2 Connect to instance untuk menghubungkan desktop jarak jauh ke instans Anda.

Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory

Prosedur ini menggabungkan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola. Jika Anda perlu melakukan gabungan domain tanpa batas di beberapa Akun AWS, lihatTutorial: Berbagi direktori Microsoft AD AWS Terkelola Anda untuk bergabung dengan domain EC2 yang mulus. Untuk informasi selengkapnya tentang Amazon EC2, lihat Apa itu Amazon EC2? .

Untuk bergabung dengan instans Windows EC2 dengan mulus

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Luncurkan instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.

a. Untuk membuat key pair baru, pilih Create new key pair.

b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.

c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.

d. Pilih create key pair.

e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

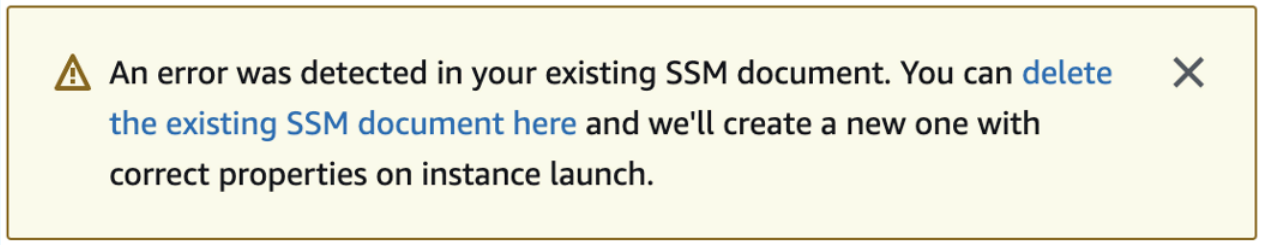
> **Important**
>
> Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

    Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:



Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:

- Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
- Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola AmazonSSM ManagedInstanceCore dan AmazonSSM yang DirectoryServiceAccess dilampirkan padanya dari daftar tarik-turun profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

    1. Pilih Buat peran.
    2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.
    3. Di bawah Kasus penggunaan, pilih EC2.
    4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih kebijakan AmazonSSM dan AmazonSSM ManagedInstanceCore. DirectoryServiceAccess Untuk memfilter daftar, **`SSM`** ketik kotak pencarian. Pilih Berikutnya.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan

kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

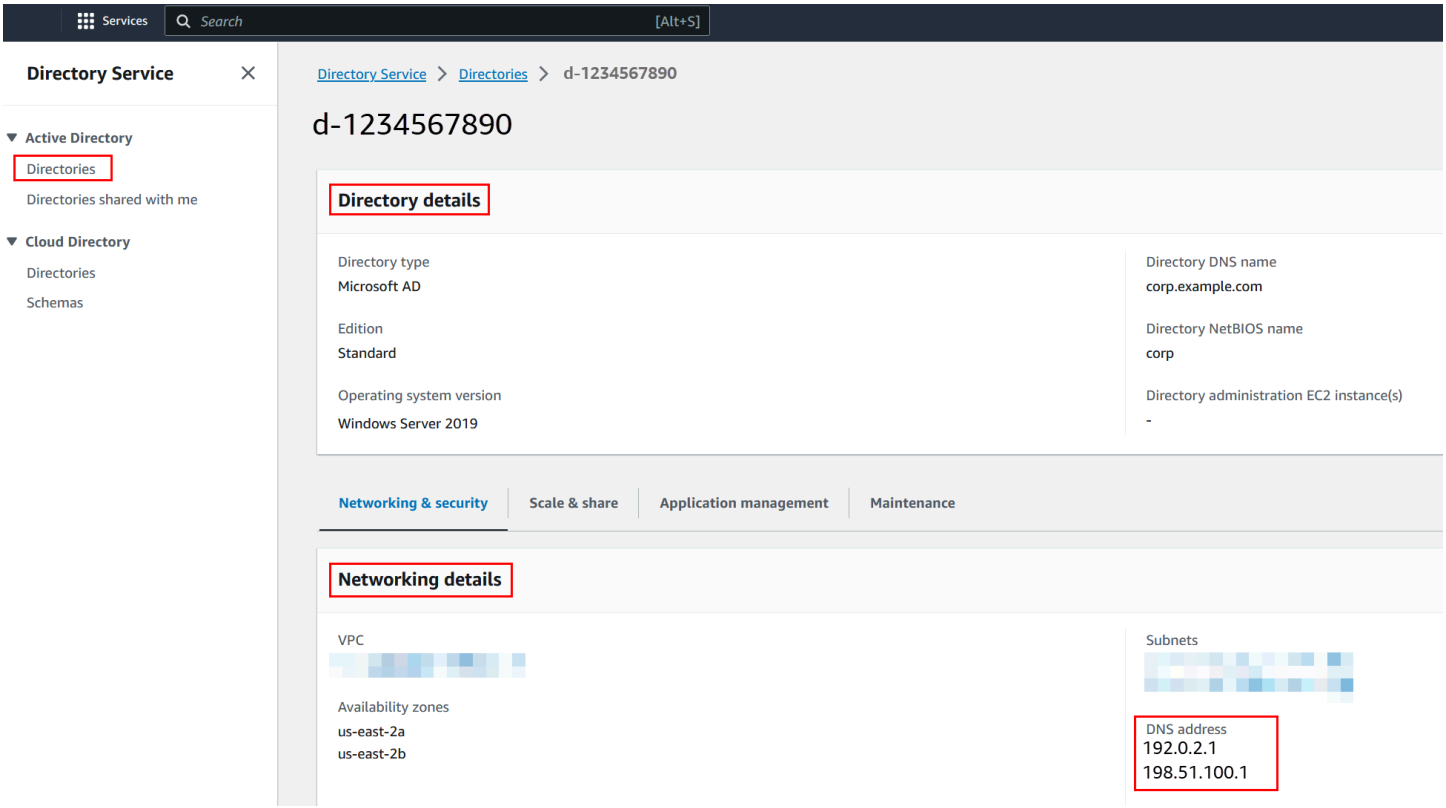
5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
7. Pilih Buat peran.
8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.

16. Pilih Luncurkan instans.

Menggabungkan instans Windows Amazon EC2 secara manual ke Direktori Aktif AWS Microsoft AD Terkelola

Untuk menggabungkan instans Amazon EC2 yang ada secara manual ke AWS Microsoft AD yang Active Directory Dikelola, instans harus diluncurkan menggunakan parameter seperti yang ditentukan dalam. Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory

Anda akan memerlukan alamat IP dari server DNS Microsoft AD yang AWS Dikelola. Informasi ini dapat ditemukan di bawah Layanan Direktori > Direktori > tautan ID Direktori untuk direktori Anda> Detail direktori dan bagian Jaringan & Keamanan.



Untuk menggabungkan instans Windows ke Microsoft AD yang AWS Dikelola Active Directory

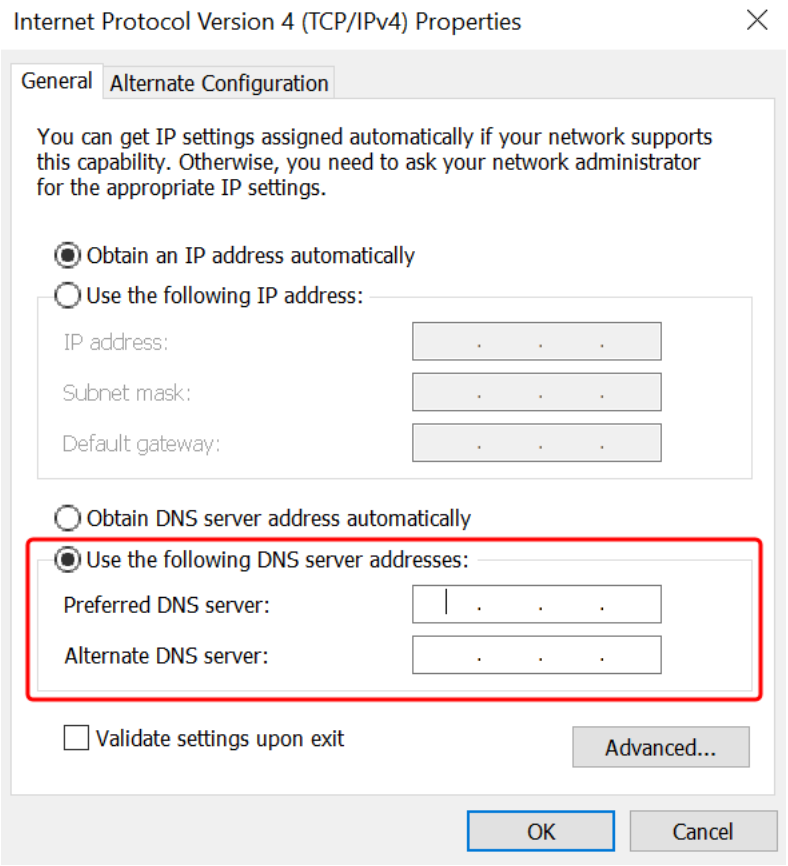
1. Connect ke instans menggunakan klien Remote Desktop Protocol.
2. Buka kotak dialog properti TCP/IPv4 pada instans.

   a. Buka Koneksi Jaringan.

   > **Tip**
   >
   > Anda dapat membuka Koneksi Jaringan langsung dengan menjalankan hal berikut dari prompt perintah pada instans.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Buka menu konteks (klik kanan) untuk koneksi jaringan yang aktif mana pun dan pilih Properti .

   c. Dalam kotak dialog properti koneksi, buka (klik dua kali) Protokol Internet Versi 4.
3. Pilih Gunakan alamat server DNS berikut, ubah server DNS pilihan dan alamat server DNS alternatif ke alamat IP server DNS yang disediakan AWS Microsoft Ad-provided, dan pilih OK.



4. Buka kotak dialog Properti Sistem untuk instans, pilih tab Nama Komputer, dan pilih Ubah.

> **Tip**
>
> Anda dapat membuka kotak dialog Properti Sistem langsung dengan menjalankan hal berikut dari prompt perintah pada instans.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Di bidang Anggota, pilih Domain, masukkan nama yang sepenuhnya memenuhi syarat dari Direktori Aktif Microsoft AD AWS Terkelola Anda, dan pilih OK.
6. Saat diminta nama dan kata sandi untuk administrator domain, masukkan nama pengguna dan kata sandi akun yang memiliki hak istimewa bergabung domain. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

> **Note**
>
> Anda dapat memasukkan nama domain yang sepenuhnya memenuhi syarat atau nama NetBIOS, diikuti dengan garis miring terbalik (\), dan kemudian nama pengguna. Nama pengguna akan menjadi Admin. Misalnya, **`corp.example.com\admin`** atau **`corp\admin`**.

7. Setelah Anda menerima pesan yang menyambut Anda ke domain, mulai ulang instans agar perubahan berlaku.

Sekarang instans Anda telah bergabung ke domain Direktori Aktif Microsoft AD AWS Terkelola, Anda dapat masuk ke instance tersebut dari jarak jauh dan menginstal utilitas untuk mengelola direktori, seperti menambahkan pengguna dan grup. Alat Administrasi Direktori Aktif dapat digunakan untuk membuat pengguna dan grup. Untuk informasi selengkapnya, lihat Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola.

> **Note**
>
> Anda juga dapat menggunakan Amazon Route 53 untuk memproses kueri DNS alih-alih mengubah alamat DNS secara manual di instans Amazon EC2 Anda. Untuk informasi selengkapnya, lihat Mengintegrasikan resolusi DNS Layanan Direktori Anda dengan Amazon Route 53 Resolver dan Meneruskan kueri DNS keluar ke jaringan Anda.

Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AWS AD Terkelola

Prosedur ini menggabungkan instans Amazon EC2 Linux dengan mulus ke Direktori Aktif Microsoft AD AWS Terkelola Anda. Jika Anda perlu melakukan gabungan domain tanpa batas di beberapa AWS akun, Anda dapat memilih untuk mengaktifkan Berbagi direktori.

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS

- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 tidak mendukung fitur penggabungan domain mulus.

Untuk demonstrasi tentang proses menggabungkan instans Linux dengan mulus ke Direktori Aktif AWS Microsoft AD Terkelola, lihat video berikut YouTube .

Amazon EC2 untuk Linux domain AD mulus bergabung dengan demo

Prasyarat

Sebelum Anda dapat mengatur gabungan domain tanpa batas ke instance Linux, Anda harus menyelesaikan prosedur di bagian ini.

Pilih akun layanan penggabungan domain mulus Anda

Anda dapat menggabungkan komputer Linux dengan mulus ke domain Direktori Aktif Microsoft AD yang AWS Dikelola. Untuk melakukannya, Anda harus membuat akun pengguna dengan membuat izin akun komputer untuk menggabungkan komputer ke domain. Meskipun anggota administrator yang didelegasikan AWS atau grup lain mungkin memiliki hak istimewa yang memadai untuk menggabungkan komputer ke domain, kami tidak menyarankan untuk menggunakan ini. Sebagai praktik terbaik, kami rekomendasikan Anda menggunakan akun layanan yang memiliki hak istimewa minimum yang diperlukan untuk menggabungkan komputer ke domain.

Untuk mendelegasikan akun dengan hak istimewa minimum yang diperlukan untuk bergabung dengan komputer ke domain, Anda dapat menjalankan perintah berikut PowerShell . Anda harus menjalankan perintah ini dari komputer Windows menggabungkan domain dengan Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola yang diinstal. Selain itu, Anda harus menggunakan akun yang memiliki izin untuk mengubah izin di OU komputer atau kontainer Anda. PowerShell Perintah menetapkan izin yang memungkinkan akun layanan untuk membuat objek komputer di wadah komputer default domain Anda.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
```

```
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Jika Anda lebih suka menggunakan antarmuka pengguna grafis (GUI) Anda dapat menggunakan proses manual yang dijelaskan di Mendelegasikan hak istimewa ke akun layanan Anda.

Membuat rahasia untuk menyimpan akun layanan domain

Anda dapat menggunakan AWS Secrets Manager untuk menyimpan akun layanan domain.

Untuk Membuat rahasia dan menyimpan informasi akun layanan domain

1. Masuk ke AWS Management Console dan buka AWS Secrets Manager konsol di https://console.aws.amazon.com/secretsmanager/.
2. Pilih Simpan rahasia baru.
3. Pada halaman Simpan rahasia baru, lakukan hal berikut:

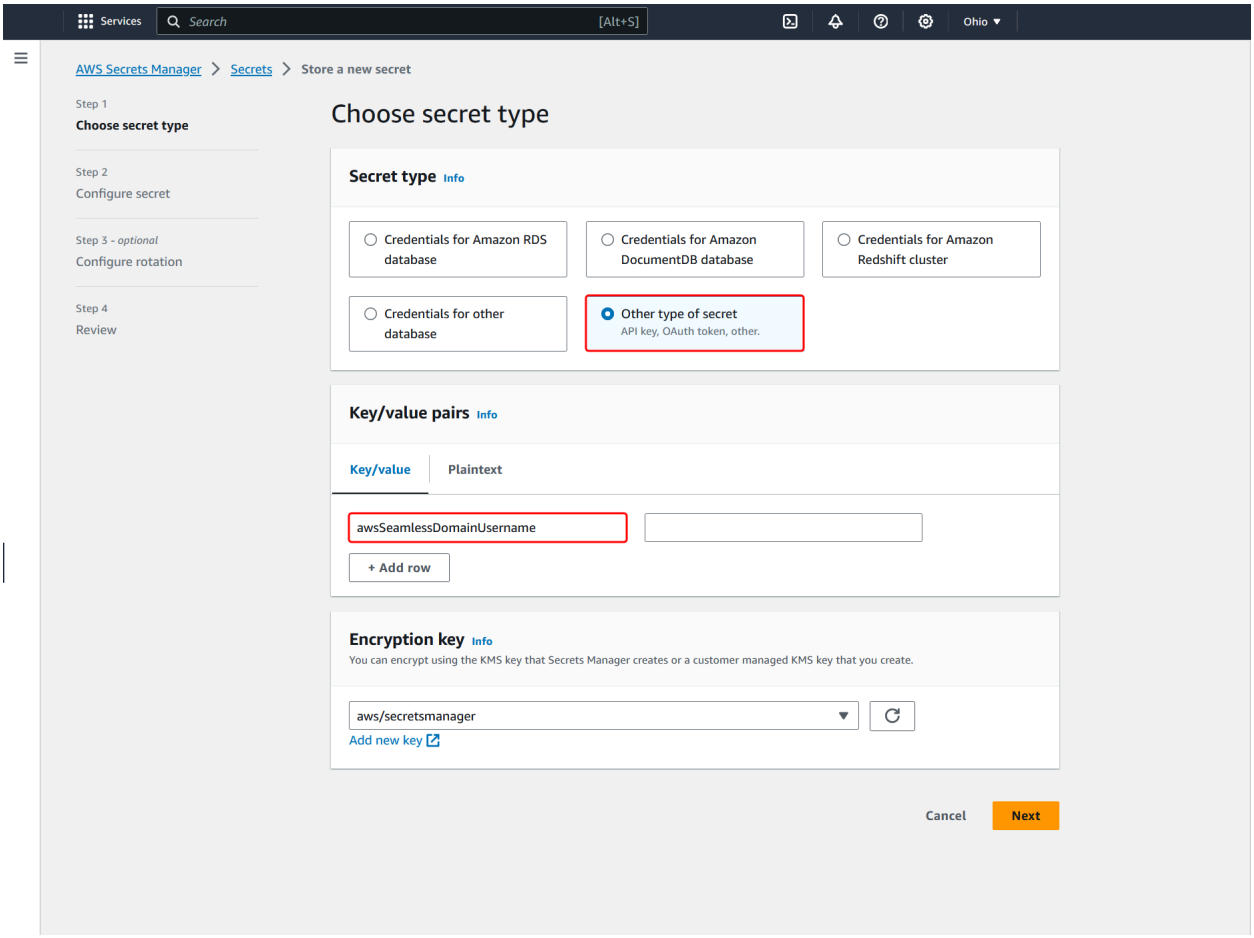
    a. Di bawah Tipe rahasia, pilih Jenis rahasia lainnya.

    b. Di bawah pasangan kunci/nilai, lakukan hal berikut:

        i. Dalam kotak pertama, masukkan **`awsSeamlessDomainUsername`**. Pada baris yang sama, di kotak berikutnya, masukkan nama pengguna untuk akun layanan Anda.

Misalnya, jika Anda menggunakan PowerShell perintah sebelumnya, nama akun layanan akan menjadi**`awsSeamlessDomain`**.

> **Note**
>
> Anda harus memasukkan **`awsSeamlessDomainUsername`** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.



ii. Pilih Tambahkan baris.

iii. Pada baris baru, di kotak pertama, masukkan **`awsSeamlessDomainPassword`**. Pada baris yang sama, di kotak berikutnya, masukkan kata sandi untuk akun layanan Anda.

> **Note**
>
> Anda harus memasukkan **awsSeamlessDomainPassword** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

iv. Di bawah kunci Enkripsi, tinggalkan nilai defaultaws/secretsmanager. AWS Secrets Manager selalu mengenkripsi rahasia ketika Anda memilih opsi ini. Anda juga dapat memilih kunci yang Anda buat.

> **Note**
>
> Ada biaya yang terkait AWS Secrets Manager, tergantung pada rahasia yang Anda gunakan. Untuk daftar harga lengkap saat ini, lihat AWS Secrets Manager Harga.
> Anda dapat menggunakan kunci AWS terkelola aws/secretsmanager yang dibuat Secrets Manager untuk mengenkripsi rahasia Anda secara gratis. Jika Anda membuat kunci KMS Anda sendiri untuk mengenkripsi rahasia Anda, AWS menagih Anda dengan tarif saat ini AWS KMS . Untuk informasi selengkapnya, silakan lihat Harga AWS Key Management Service.

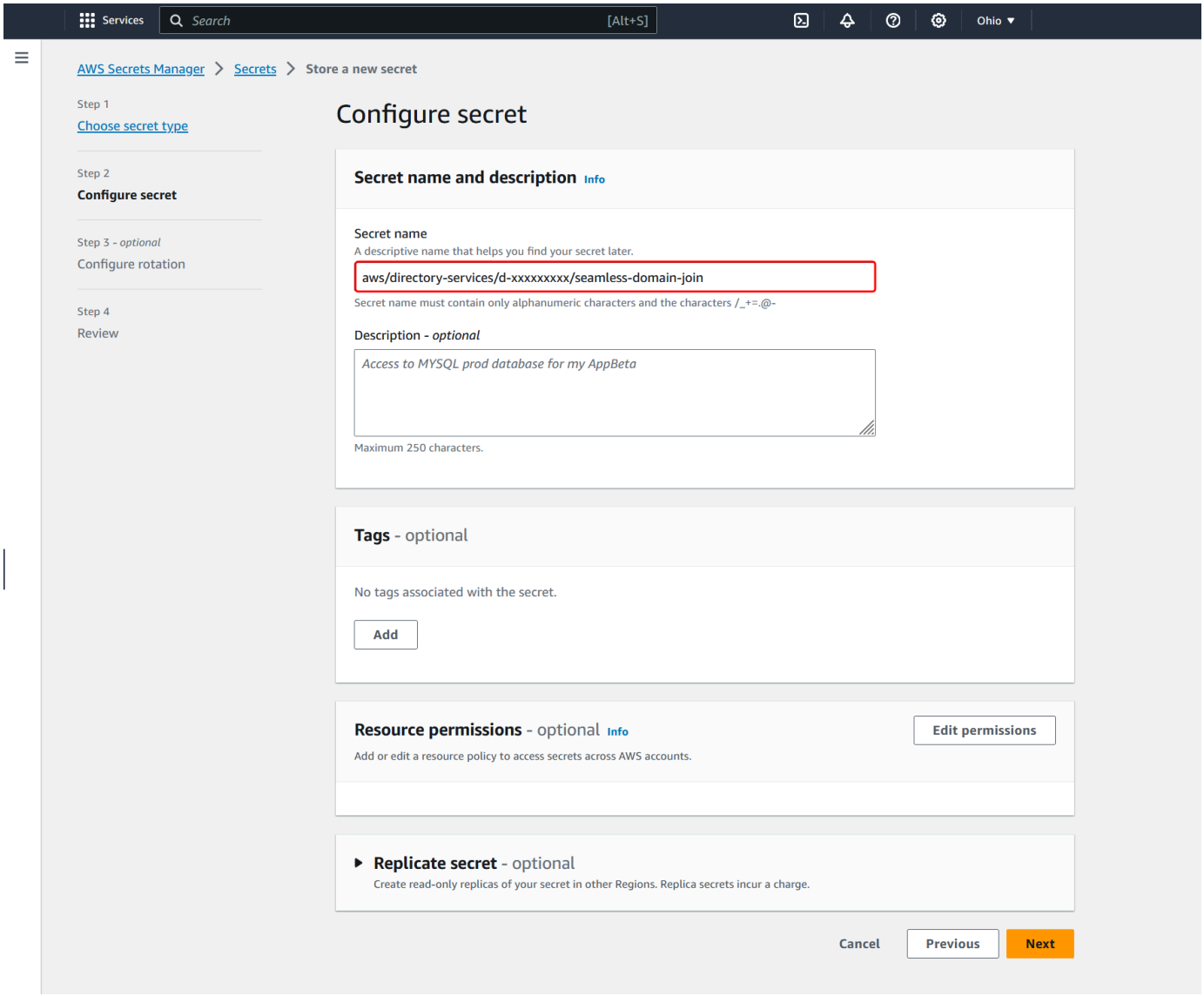
v. Pilih Berikutnya.

4. Di bawah nama Rahasia, masukkan nama rahasia yang menyertakan ID direktori Anda menggunakan format berikut, ganti *d-xxxxxxxxx* dengan ID direktori Anda:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Ini akan digunakan untuk mengambil rahasia dalam aplikasi.

> **Note**
>
> Anda harus memasukkan **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** persis seperti itu tapi ganti *d-xxxxxxxxx* dengan ID direktori Anda. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.



5. Biarkan yang lainnya diatur ke default, dan kemudian pilih Selanjutnya.
6. Di bawah Konfigurasikan rotasi otomatis, pilih Nonaktifkan rotasi otomatis, lalu pilih Selanjutnya.
7. Tinjau pengaturan, dan kemudian pilih Simpan untuk menyimpan perubahan Anda. Konsol Secrets Manager mengembalikan Anda ke daftar rahasia di akun Anda dengan rahasia baru Anda masuk di dalam daftar.
8. Pilih nama rahasia Anda yang baru dibuat dari daftar, dan perhatikan nilai ARN rahasia. Anda akan membutuhkannya di bagian selanjutnya.

Untuk membuat kebijakan dan peran IAM yang diperlukan

Gunakan langkah-langkah prasyarat berikut untuk membuat kebijakan khusus yang memungkinkan akses hanya-baca ke rahasia gabungan domain tanpa batas Secrets Manager Anda (yang Anda buat sebelumnya), dan untuk membuat peran IAM LinuxEC2 baru. DomainJoin

Membuat kebijakan membaca IAM Secrets Manager

Anda menggunakan konsol IAM untuk membuat kebijakan yang memberikan akses hanya-baca ke rahasia Secrets Manager Anda.

Untuk membuat kebijakan membaca IAM Secrets Manager

1. Masuk ke pengguna AWS Management Console sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Lalu buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, Manajemen Akses, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pilih tab JSON dan salin teks dari dokumen kebijakan JSON berikut. Kemudian tempelkan ke dalam kotak teks JSON.

> **Note**
>
> Pastikan Anda mengganti Region and Resource ARN dengan Region dan ARN sebenarnya dari rahasia yang Anda buat sebelumnya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
```

```
    ]
}
```

5. Setelah selesai, pilih Selanjutnya. Validator kebijakan melaporkan kesalahan sintaksis. Untuk informasi selengkapnya, lihat Memvalidasi kebijakan IAM.
6. Pada halaman Tinjau kebijakan, masukkan nama kebijakan, seperti **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`**. Tinjau bagian Ringkasan untuk melihat izin yang diberikan oleh kebijakan Anda. Lalu pilih Buat kebijakan untuk menyimpan perubahan Anda. Kebijakan baru muncul di daftar kebijakan terkelola dan siap dilampirkan pada identitas.

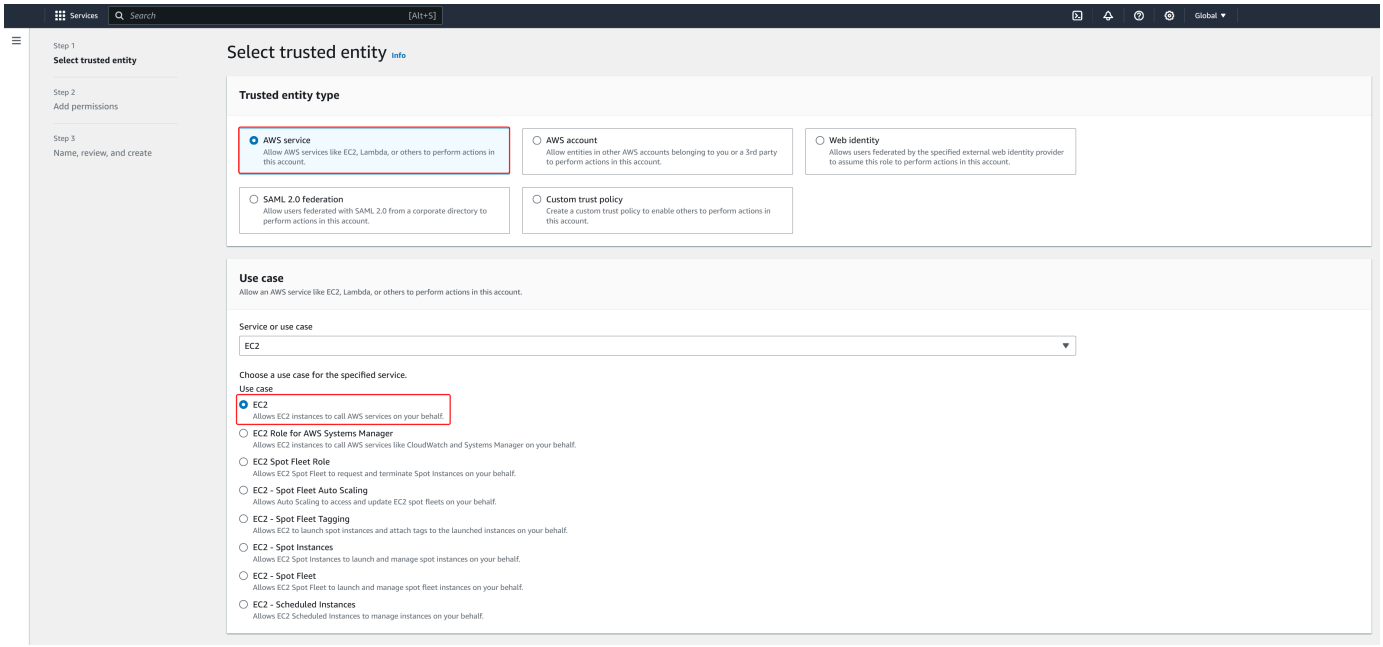
> **Note**
>
> Kami rekomendasikan Anda membuat satu kebijakan per rahasia. Melakukan hal tersebut memastikan bahwa instans hanya memiliki akses ke rahasia yang sesuai dan meminimalkan dampak jika sebuah instans dikompromikan.

Buat peran LinuXEC2 DomainJoin

Anda menggunakan konsol IAM untuk membuat peran yang akan Anda gunakan untuk penggabungan domain dengan instans EC2 Linux Anda.

Untuk membuat peran LinuXEC2 DomainJoin

1. Masuk ke pengguna AWS Management Console sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Lalu buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, di bawah Manajemen Akses, pilih Peran.
3. Di panel konten, pilih Buat peran.
4. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
5. Di bawah Kasus penggunaan, pilih EC2, lalu pilih Berikutnya.



6. Untuk Kebijakan filter, lakukan hal berikut:

   a. Masukkan **`AmazonSSMManagedInstanceCore`**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   b. Masukkan **`AmazonSSMDirectoryServiceAccess`**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   c. Masukkan **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (atau nama kebijakan yang Anda buat dalam prosedur sebelumnya). Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   d. Setelah menambahkan tiga kebijakan yang tercantum di atas, pilih Buat peran.

> **Note**
>
> AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory Service AmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

7. Masukkan nama untuk peran baru Anda, seperti **`LinuxEC2DomainJoin`** atau nama lain yang Anda inginkan di bidang Nama peran.
8. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
9. (Opsional) Pilih Tambahkan tag baru di bawah Langkah 3: Tambahkan tag untuk menambahkan tag. Pasangan nilai kunci tag digunakan untuk mengatur, melacak, atau mengontrol akses untuk peran ini.
10. Pilih Buat peran.

Bergabunglah dengan instans Linux Anda dengan mulus

Sekarang setelah Anda mengonfigurasi semua tugas prasyarat, Anda dapat menggunakan prosedur berikut untuk bergabung dengan instans Linux EC2 Anda dengan mulus.

Untuk bergabung dengan instans Linux Anda dengan mulus

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Dari pemilih Region di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Name and Tags, masukkan nama yang ingin Anda gunakan untuk instans Linux EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih AMI Linux yang ingin Anda luncurkan.

> **Note**
>
> AMI yang digunakan harus memiliki AWS Systems Manager (Agen SSM) versi 2.3.1644.0 atau lebih tinggi. Untuk memeriksa versi SSM Agent yang diinstal di AMI Anda dengan meluncurkan sebuah instans dari AMI tersebut, lihat Mendapatkan versi Agen SSM yang saat ini diinstal. Jika Anda perlu meningkatkan Agen SSM, lihat Menginstal dan mengkonfigurasi SSM Agent pada instans EC2 untuk Linux.
> SSM menggunakan `aws:domainJoin` plugin saat menggabungkan instance Linux ke Active Directory domain. *`Plugin mengubah nama host untuk instance Linux ke format EC2AMAZ- XXXXXXX.`* Untuk informasi selengkapnya`aws:domainJoin`,

lihat referensi plugin dokumen AWS Systems Manager perintah di Panduan AWS Systems Manager Pengguna.

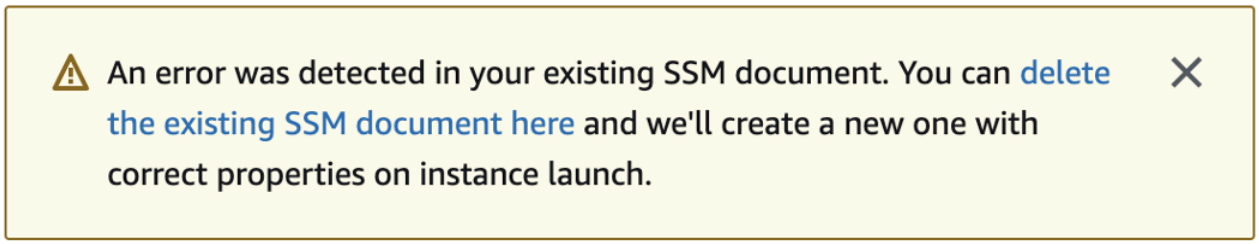
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada. Untuk membuat key pair baru, pilih Create new key pair. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk. Pilih create key pair. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

   ⚠ Important

   Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.
9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

    Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:
>
> 
>
>
> Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:
>
> - Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
> - Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, pilih peran IAM yang sebelumnya Anda buat di bagian prasyarat Langkah 2: Buat peran LinuxEC2. DomainJoin
16. Pilih Luncurkan instans.

> **Note**
>
> Jika Anda menjalankan penggabungan domain yang mulus dengan SUSE Linux, reboot diperlukan sebelum autentikasi akan bekerja. Untuk me-reboot SUSE dari terminal Linux, ketik sudo reboot.

Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola

Selain instans Windows Amazon EC2, Anda juga dapat menggabungkan instans Amazon EC2 Linux tertentu ke Direktori Aktif Microsoft AD AWS Terkelola. Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Distribusi dan versi Linux lainnya mungkin bekerja namun belum diuji.

Bergabunglah dengan instans Linux ke Microsoft AD yang AWS Dikelola

Sebelum Anda dapat menggabungkan instans Amazon Linux, CentOS, Red Hat, atau Ubuntu ke direktori Anda, instans harus terlebih dahulu diluncurkan sebagaimana ditentukan dalam Bergabunglah dengan instans Linux Anda dengan mulus.

> **Important**
>
> Beberapa prosedur berikut, jika tidak dilakukan dengan benar, dapat membuat instans anda tidak terjangkau atau tidak dapat digunakan. Oleh karena itu, kami sangat menyarankan Anda membuat backup atau mengambil snapshot dari instans Anda sebelum melakukan prosedur ini.

Untuk bergabung dengan instance Linux ke direktori Anda

Ikuti langkah-langkah untuk instans Linux tertentu Anda menggunakan salah satu tab berikut:

Amazon Linux

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya

di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Amazon Linux - 64bit Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Amazon Linux yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Untuk bantuan dalam menentukan versi Amazon Linux yang Anda gunakan, lihat Mengidentifikasi image Amazon Linux dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Akun pada domain *example.com* yang memiliki hak istimewa untuk penggabungan domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.
   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

7. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:
   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

CentOS

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans CentOS 7 Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket CentOS 7 yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Akun pada domain *example.com* yang memiliki hak istimewa untuk penggabungan domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

7. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

Red Hat

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Red Hat - 64bit adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Red Hat yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

SAM AccountName untuk akun di domain *example.com* yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
```

```
* Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

7. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

SUSE

1. Terhubung ke instans menggunakan klien SSH apa saja.

2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan AWS Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans SUSE Linux 15 Anda adalah yang terbaru.

   a. Hubungkan repositori paket.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Pembaruan SUSE.

   ```
   sudo zypper update -y
   ```

4. Instal paket SUSE Linux 15 yang diperlukan pada instans Linux Anda.

   > **Note**
   >
   > Beberapa paket ini mungkin sudah diinstal.
   > Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

   ```
   sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
   ```

5. Menggabungkan instans ke direktori dengan perintah berikut.

   ```
   sudo realm join -U join_account example.com --verbose
   ```

   join_account

   SAM AccountName di domain *example.com* yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Perhatikan bahwa kedua pengembalian berikut diharapkan.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Mengaktifkan SSSD di PAM secara manual.

```
sudo pam-config --add --sss
```

7. Edit nsswitch.conf untuk mengaktifkan SSSD di nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Tambahkan baris berikut ke /etc/pam.d/common-session untuk membuat direktori home secara otomatis pada login awal.

```
sudo vi /etc/pam.d/common-session
```

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Reboot instans untuk menyelesaikan proses penggabungan domain.

```
sudo reboot
```

10. Hubungkan kembali ke instans menggunakan klien SSH untuk memverifikasi bergabung domain telah berhasil diselesaikan dan menyelesaikan langkah-langkah tambahan.

    a. Untuk mengkonfimasi instans telah didaftarkan pada domain

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

b. Untuk memverifikasi status daemon SSSD

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
           ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
           ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. Untuk mengizinkan akses pengguna melalui SSH dan konsol

```
sudo realm permit join_account@example.com
```

Untuk mengizinkan akses grup domain melalui SSH dan konsol

```
sudo realm permit -g 'AWS Delegated Administrators'
```

Atau untuk mengizinkan semua pengguna mengakses

```
sudo realm permit --all
```

12. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

    a. Buka file `/etc/ssh/sshd_config` di editor teks.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Atur pengaturan `PasswordAuthentication` ke `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Mulai ulang layanan SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    Atau:

    ```
    sudo service sshd restart
    ```

13. 13. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:

    a. Buka file sudoers dengan perintah berikut:

    ```
    sudo visudo
    ```

    b. Tambahkan hal berikut ini ke bagian bawah file sudoers dan simpan.

    ```
    ## Add the "Domain Admins" group from the awsad.com domain.
    %AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
    ```

Ubuntu

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Ubuntu - 64bit Anda adalah yang terbaru.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Instal paket Ubuntu yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Nonaktifkan resolusi Reverse DNS dan atur ranah default ke FQDN domain Anda. Instans Ubuntu harus dapat dipecahkan terbalik di DNS sebelum ranah akan bekerja. Jika tidak, Anda harus menonaktifkan DNS terbalik di /etc/krb5.conf sebagai berikut:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

SAM AccountName untuk akun di domain *example.com* yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

7. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.
   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

8. Setelah instance dimulai ulang, sambungkan dengan klien SSH apa pun dan tambahkan grup Administrator AWS Delegasi ke daftar sudoers dengan melakukan langkah-langkah berikut:
   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   ```

```
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

Membatasi akses login akun

Karena semua akun ditetapkan dalam Direktori Aktif, secara default, semua pengguna dalam direktori tersebut dapat masuk ke instans. Anda dapat mengizinkan hanya pengguna tertentu untuk masuk ke instans dengan ad_access_filter di sssd.conf. Sebagai contoh:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Menunjukkan bahwa pengguna hanya boleh diizinkan akses ke instans jika mereka adalah anggota dari grup tertentu.

cn

Nama umum grup yang harus memiliki akses. Dalam contoh ini, nama grupnya adalah *admins*.

ou

Ini adalah unit organisasi tempat grup di atas berada. Dalam contoh ini, OU adalah *Testou*.

dc

Ini adalah komponen domain dari domain Anda. Dalam contoh ini, *example*.

dc

Ini adalah komponen domain tambahan. Dalam contoh ini, *com*.

Anda harus menambahkan ad_access_filter secara manual ke /etc/sssd/sssd.conf.

Buka file /etc/sssd/sssd.conf di editor teks.

```
sudo vi /etc/sssd/sssd.conf
```

Setelah melakukan hal ini, sssd.conf Anda mungkin terlihat seperti ini:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Agar konfigurasi mulai berlaku, Anda perlu memulai ulang layanan sssd:

```
sudo systemctl restart sssd.service
```

Atau, Anda dapat menggunakan .

```
sudo service sssd restart
```

Karena semua akun ditetapkan dalam Direktori Aktif, secara default, semua pengguna dalam direktori tersebut dapat masuk ke instans. Anda dapat mengizinkan hanya pengguna tertentu untuk masuk ke instans dengan ad_access_filter di sssd.conf.

Sebagai contoh:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Menunjukkan bahwa pengguna hanya boleh diizinkan akses ke instans jika mereka adalah anggota dari grup tertentu.

cn

Nama umum grup yang harus memiliki akses. Dalam contoh ini, nama grupnya adalah *admins*.

ou

Ini adalah unit organisasi tempat grup di atas berada. Dalam contoh ini, OU adalah *Testou*.

dc

Ini adalah komponen domain dari domain Anda. Dalam contoh ini, *example*.

dc

Ini adalah komponen domain tambahan. Dalam contoh ini, *com*.

Anda harus menambahkan ad_access_filter secara manual ke /etc/sssd/sssd.conf.

1. Buka file /etc/sssd/sssd.conf di editor teks.

```
sudo vi /etc/sssd/sssd.conf
```

2. Setelah melakukan hal ini, sssd.conf Anda mungkin terlihat seperti ini:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. Agar konfigurasi mulai berlaku, Anda perlu memulai ulang layanan sssd:

```
sudo systemctl restart sssd.service
```

Atau, Anda dapat menggunakan .

```
sudo service sssd restart
```

Pemetaan ID

Pemetaan ID dapat dilakukan dengan dua metode untuk mempertahankan pengalaman terpadu antara identitas UNIX/Linux User Identifier (UID) dan Group Identifier (GID) dan Windows and Security Identifier (SID). Active Directory

1. Terpusat
2. Didistribusikan

> **Note**
>
> Pemetaan identitas pengguna terpusat di Active Directory memerlukan Antarmuka Sistem Operasi Portabel atau POSIX.

Pemetaan identitas pengguna terpusat

Active Directoryatau layanan Lightweight Directory Access Protocol (LDAP) lainnya menyediakan UID dan GID kepada pengguna Linux. DalamActive Directory, pengidentifikasi ini disimpan dalam atribut pengguna:

- UID - Nama pengguna Linux (String)
- Nomor UID - Nomor ID Pengguna Linux (Integer)
- Nomor GID - Nomor ID Grup Linux (Integer)

Untuk mengkonfigurasi instance Linux untuk menggunakan UID dan GID dariActive Directory, atur `ldap_id_mapping = False` dalam file sssd.conf. Sebelum menyetel nilai ini, verifikasi bahwa Anda telah menambahkan UID, nomor UID, dan nomor GID ke pengguna dan grup. Active Directory

Pemetaan identitas pengguna terdistribusi

Jika Active Directory tidak memiliki ekstensi POSIX atau jika Anda memilih untuk tidak mengelola pemetaan identitas secara terpusat, Linux dapat menghitung nilai UID dan GID. Linux menggunakan Security Identifier (SID) unik pengguna untuk menjaga konsistensi.

Untuk mengonfigurasi pemetaan ID pengguna terdistribusi, atur `ldap_id_mapping = True` dalam file sssd.conf.

Connect ke instance Linux

Ketika pengguna terhubung ke instance menggunakan klien SSH, mereka diminta untuk nama pengguna mereka. Pengguna dapat memasukkan nama pengguna dalam `EXAMPLE\username` format `username@example.com` atau. Respons akan muncul mirip dengan yang berikut ini, tergantung pada distribusi Linux yang Anda gunakan:

Amazon Linux, Red Hat Enterprise Linux, dan CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
```

```
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Menggabungkan instans Amazon EC2 Linux secara manual ke Direktori Aktif AWS Microsoft AD Terkelola menggunakan Winbind

Anda dapat menggunakan layanan Winbind untuk menggabungkan instans Amazon EC2 Linux secara manual ke domain Direktori Aktif Microsoft AD AWS Terkelola. Ini memungkinkan pengguna Active Directory lokal Anda yang ada untuk menggunakan kredenal Direktori Aktif mereka saat mengakses instance Linux yang bergabung dengan Direktori Aktif AWS Microsoft AD Terkelola Anda. Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Distribusi dan versi Linux lainnya mungkin bekerja namun belum diuji.

Bergabunglah dengan instans Linux ke Direktori Aktif Microsoft AD AWS Terkelola

> **Important**
>
> Beberapa prosedur berikut, jika tidak dilakukan dengan benar, dapat membuat instans anda tidak terjangkau atau tidak dapat digunakan. Oleh karena itu, kami sangat menyarankan

Anda membuat backup atau mengambil snapshot dari instans Anda sebelum melakukan prosedur ini.

Untuk bergabung dengan instance Linux ke direktori Anda

Ikuti langkah-langkah untuk instans Linux tertentu Anda menggunakan salah satu tab berikut:

Amazon Linux/CENTOS/REDHAT

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan AWS Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Linux Anda adalah yang terbaru.

   ```
   sudo yum -y update
   ```

4. Instal paket Samba / Winbind yang diperlukan pada instans Linux Anda.

   ```
   sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
   ```

5. Buat backup dari file `smb.conf` utama sehingga Anda dapat kembali ke sana jika terjadi kegagalan:

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. Buka file konfigurasi [`/etc/samba/smb.conf`] asli di editor teks.

   ```
   sudo vim /etc/samba/smb.conf
   ```

   Isi informasi lingkungan domain Active Directory Anda seperti yang ditunjukkan pada contoh di bawah ini:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Buka file host [`/etc/hosts`] di editor teks.

```
sudo vim /etc/hosts
```

Tambahkan alamat IP privat instans Linux Anda sebagai berikut:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Jika Anda tidak menentukan alamat IP Anda di file `/etc/hosts`, Anda mungkin menerima error DNS berikut saat menggabungkan instans ke domain.:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Error ini berarti bahwa penggabungan berhasil tetapi perintah [net ads] tidak dapat mendaftarkan catatan DNS di DNS.

8. Menggabungkan instans Linux ke Direktori Aktif menggunakan utilitas net.

```
sudo net ads join -U join_account@example.com
```

`join_account@example.com`

Akun pada domain *`example.com`* yang memiliki hak istimewa untuk penggabungan domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya

tentang mendelegasikan hak istimewa ini, lihat [Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS](#).

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Memodifikasi file konfigurasi PAM, Gunakan perintah di bawah ini untuk menambahkan entri yang diperlukan untuk autentikasi winbind:

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi dengan mengedit file `/etc/ssh/sshd_config`.

    a. Buka file `/etc/ssh/sshd_config` di editor teks.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Atur pengaturan `PasswordAuthentication` ke `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Mulai ulang layanan SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    Atau:

    ```
    sudo service sshd restart
    ```

11. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH dan tambahkan hak istimewa root untuk pengguna atau grup domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

    a. Buka file `sudoers` dengan perintah berikut:

    ```
    sudo visudo
    ```

b. Tambahkan grup atau pengguna yang diperlukan dari domain Trusting atau Trusted sebagai berikut, dan kemudian simpan.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

SUSE

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan AWS Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans SUSE Linux 15 Anda adalah yang terbaru.
   a. Hubungkan repositori paket.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Pembaruan SUSE.

   ```
   sudo zypper update -y
   ```

4. Instal paket Samba / Winbind yang diperlukan pada instans Linux Anda.

   ```
   sudo zypper in -y samba samba-winbind
   ```

5. Buat backup dari file `smb.conf` utama sehingga Anda dapat kembali ke sana jika terjadi kegagalan:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Buka file konfigurasi [`/etc/samba/smb.conf`] asli di editor teks.

```
sudo vim /etc/samba/smb.conf
```

Isi informasi lingkungan domain direktori Aktif Anda seperti yang ditunjukkan pada contoh di bawah ini:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Buka file host [`/etc/hosts`] di editor teks.

```
sudo vim /etc/hosts
```

Tambahkan alamat IP privat instans Linux Anda sebagai berikut:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Jika Anda tidak menentukan alamat IP Anda di file `/etc/hosts`, Anda mungkin menerima error DNS berikut saat menggabungkan instans ke domain.:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Error ini berarti bahwa penggabungan berhasil tetapi perintah [net ads] tidak dapat mendaftarkan catatan DNS di DNS.

8. Menggabungkan instans Linux ke direktori dengan perintah berikut.

```
sudo net ads join -U join_account@example.com
```

join_account

SAM AccountName di domain *example.com* yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Memodifikasi file konfigurasi PAM, Gunakan perintah di bawah ini untuk menambahkan entri yang diperlukan untuk autentikasi Winbind:

```
sudo pam-config --add --winbind --mkhomedir
```

10. Buka file konfigurasi Name Service Switch [`/etc/nsswitch.conf`] di editor teks.

```
vim /etc/nsswitch.conf
```

Tambahkan direktif Winbind seperti yang ditunjukkan di bawah ini.

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi dengan mengedit file `/etc/ssh/sshd_config`.

a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vim /etc/ssh/sshd_config
```

b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

12. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH dan tambahkan hak istimewa root untuk pengguna atau grup domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

a. Buka file `sudoers` dengan perintah berikut:

```
sudo visudo
```

b. Tambahkan grup atau pengguna yang diperlukan dari domain Trusting atau Trusted sebagai berikut, dan kemudian simpan.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

Ubuntu

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Mengkonfigurasi instans Linux untuk menggunakan alamat IP server DNS dari server DNS yang disediakan AWS Directory Service. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada

instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 pribadi di AWS Pusat Pengetahuan untuk panduan tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Linux Anda adalah yang terbaru.

```
sudo yum -y update
```

```
sudo apt-get -y upgrade
```

4. Instal paket Samba / Winbind yang diperlukan pada instans Linux Anda.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. Buat backup dari file `smb.conf` utama sehingga Anda dapat kembali ke sana jika terjadi kegagalan.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Buka file konfigurasi [`/etc/samba/smb.conf`] asli di editor teks.

```
sudo vim /etc/samba/smb.conf
```

Isi informasi lingkungan domain direktori Aktif Anda seperti yang ditunjukkan pada contoh di bawah ini:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Buka file host [`/etc/hosts`] di editor teks.

```
sudo vim /etc/hosts
```

Tambahkan alamat IP privat instans Linux Anda sebagai berikut:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Jika Anda tidak menentukan alamat IP Anda di file `/etc/hosts`, Anda mungkin menerima error DNS berikut saat menggabungkan instans ke domain.:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Error ini berarti bahwa penggabungan berhasil tetapi perintah [net ads] tidak dapat mendaftarkan catatan DNS di DNS.

8. Menggabungkan instans Linux ke Direktori Aktif menggunakan utilitas net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Akun pada domain *example.com* yang memiliki hak istimewa untuk penggabungan domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Memodifikasi file konfigurasi PAM, Gunakan perintah di bawah ini untuk menambahkan entri yang diperlukan untuk autentikasi Winbind:

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Buka file konfigurasi Name Service Switch [`/etc/nsswitch.conf`] di editor teks.

```
vim /etc/nsswitch.conf
```

Tambahkan direktif Winbind seperti yang ditunjukkan di bawah ini.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi dengan mengedit file `/etc/ssh/sshd_config`.

a. Buka file `/etc/ssh/sshd_config` di editor teks.

```
sudo vim /etc/ssh/sshd_config
```

b. Atur pengaturan `PasswordAuthentication` ke `yes`.

```
PasswordAuthentication yes
```

c. Mulai ulang layanan SSH.

```
sudo systemctl restart sshd.service
```

Atau:

```
sudo service sshd restart
```

12. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH dan tambahkan hak istimewa root untuk pengguna atau grup domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

a. Buka file `sudoers` dengan perintah berikut:

```
sudo visudo
```

b. Tambahkan grup atau pengguna yang diperlukan dari domain Trusting atau Trusted sebagai berikut, dan kemudian simpan.

```
## Adding Domain Users/Groups
```

```
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

Connect ke instance Linux

Ketika pengguna terhubung ke instance menggunakan klien SSH, mereka diminta untuk nama pengguna mereka. Pengguna dapat memasukkan nama pengguna dalam `EXAMPLE\username` format `username@example.com` atau. Respons akan muncul mirip dengan yang berikut ini, tergantung pada distribusi Linux yang Anda gunakan:

Amazon Linux, Red Hat Enterprise Linux, dan CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Menggabungkan instans Amazon EC2 Mac secara manual ke Direktori Aktif AWS Microsoft AD Terkelola

Prosedur ini secara manual menggabungkan instans Amazon EC2 Mac ke Direktori Aktif Microsoft AD AWS Terkelola Anda.

Prasyarat

- Instans Amazon EC2 Mac memerlukan Host Khusus Amazon EC2. Anda harus mengalokasikan host khusus dan meluncurkan instance ke host. Untuk informasi selengkapnya, lihat Meluncurkan instance Mac di Panduan Pengguna Amazon EC2 untuk Instans Linux.
- Sebaiknya buat set opsi DHCP untuk Direktori Aktif Microsoft AD AWS Terkelola Anda. Ini akan memungkinkan instance apa pun di VPC Amazon Anda mengarah ke domain dan server DNS yang ditentukan untuk menyelesaikan nama domain mereka. Untuk informasi selengkapnya, lihat Buat set opsi DHCP.

> **Note**
>
> Harga Dedicated Host bervariasi menurut opsi pembayaran yang Anda pilih. Untuk informasi selengkapnya, lihat Harga dan Penagihan di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Untuk bergabung dengan instance Mac secara manual

1. Gunakan perintah SSH berikut untuk terhubung ke instance Mac Anda. Untuk informasi selengkapnya tentang menghubungkan ke instans Mac, lihat Connect ke instance Mac Anda.

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

2. Setelah Anda terhubung ke instance Mac Anda, buat kata sandi untuk akun *ec2-user* menggunakan perintah berikut:

```
sudo passwd ec2-user
```

3. Saat diminta di baris perintah, berikan kata sandi untuk akun pengguna *ec2*. Anda dapat memperbarui sistem operasi dan perangkat lunak Anda dengan mengikuti prosedur di Perbarui sistem operasi dan perangkat lunak di Panduan Pengguna Amazon EC2 untuk Instans Linux.
4. Gunakan perintah *dsconfigad* berikut untuk menggabungkan instance Mac Anda ke domain Direktori Aktif AWS Microsoft AD Terkelola. Pastikan untuk mengganti nama domain, nama komputer, dan unit organisasi dengan informasi domain Microsoft AD Active Directory AWS Terkelola. Untuk informasi selengkapnya, lihat Mengonfigurasi akses domain di Utilitas Direktori di Mac di situs web Apple.

> **Warning**
>
> Nama komputer seharusnya tidak mengandung tanda hubung. Tanda hubung dapat mencegah ikatan ke Direktori Aktif AWS Microsoft AD yang Dikelola.

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

Contoh berikut adalah seperti apa perintah itu ketika bergabung dengan pengguna administratif pada instance Mac bernama **myec2mac01** **example.com** domain:

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Gunakan perintah berikut untuk menambahkan Administrator AWS Delegasi ke pengguna administratif pada instance Mac Anda:

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. Gunakan perintah berikut untuk mengonfirmasi bahwa gabungan domain Microsoft AD Active Directory AWS Terkelola berhasil:

```
dsconfigad -show
```

Anda telah berhasil menggabungkan instance Mac ke Direktori Aktif Microsoft AD AWS Terkelola. Sekarang Anda dapat masuk ke instans Mac menggunakan kredensi Direktori Aktif Microsoft AD AWS Terkelola.

Ketika Anda pertama kali masuk ke instance Mac Anda, Anda harus diberikan opsi untuk masuk sebagai pengguna “Lainnya”. Pada titik ini, Anda dapat menggunakan kredensi domain Active Directory untuk masuk ke instance Mac. Jika Anda tidak diberikan “Lainnya” di layar masuk setelah menyelesaikan langkah-langkah ini, masuk sebagai pengguna ec2 dan kemudian keluar.

Untuk masuk menggunakan antarmuka pengguna grafis dengan pengguna domain, ikuti langkah-langkah di Connect to the graphical user interface (GUI) instans Anda di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS

Untuk bergabung dengan komputer ke direktori Anda, Anda memerlukan akun yang memiliki hak istimewa untuk menggabungkan komputer ke direktori.

Dengan AWS Directory Service untuk Microsoft Active Directory, anggota grup Admin dan Administrator Server AWS Delegasi memiliki hak istimewa ini.

Namun, sebagai praktik terbaik, Anda harus menggunakan akun yang hanya memiliki hak istimewa minimum yang diperlukan. Prosedur berikut menunjukkan cara membuat grup baru yang disebut `Joiners` dan mendelegasikan hak istimewa untuk grup ini yang diperlukan untuk menggabungkan komputer ke direktori.

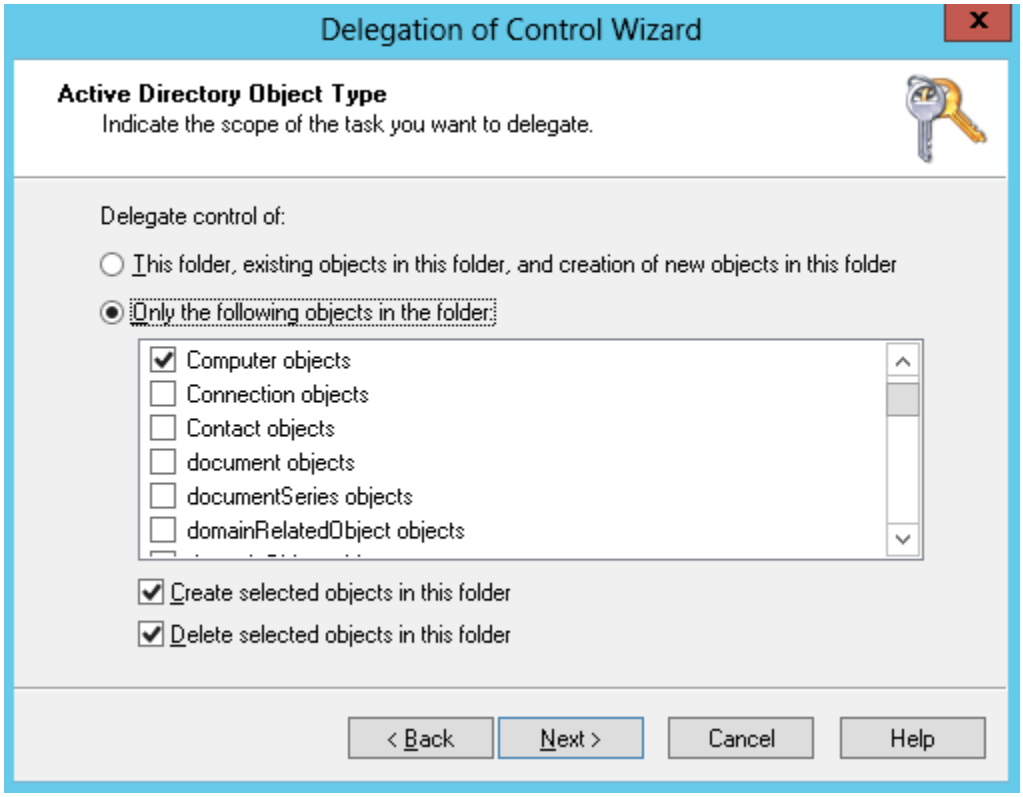
Anda harus melakukan prosedur ini pada komputer yang telah tergabung ke direktori Anda dan memiliki MMC snap-in Pengguna dan Komputer Direktori Aktif terinstal. Anda juga harus masuk sebagai administrator domain.

Untuk mendelegasikan hak istimewa bergabung untuk AWS Microsoft AD yang Dikelola

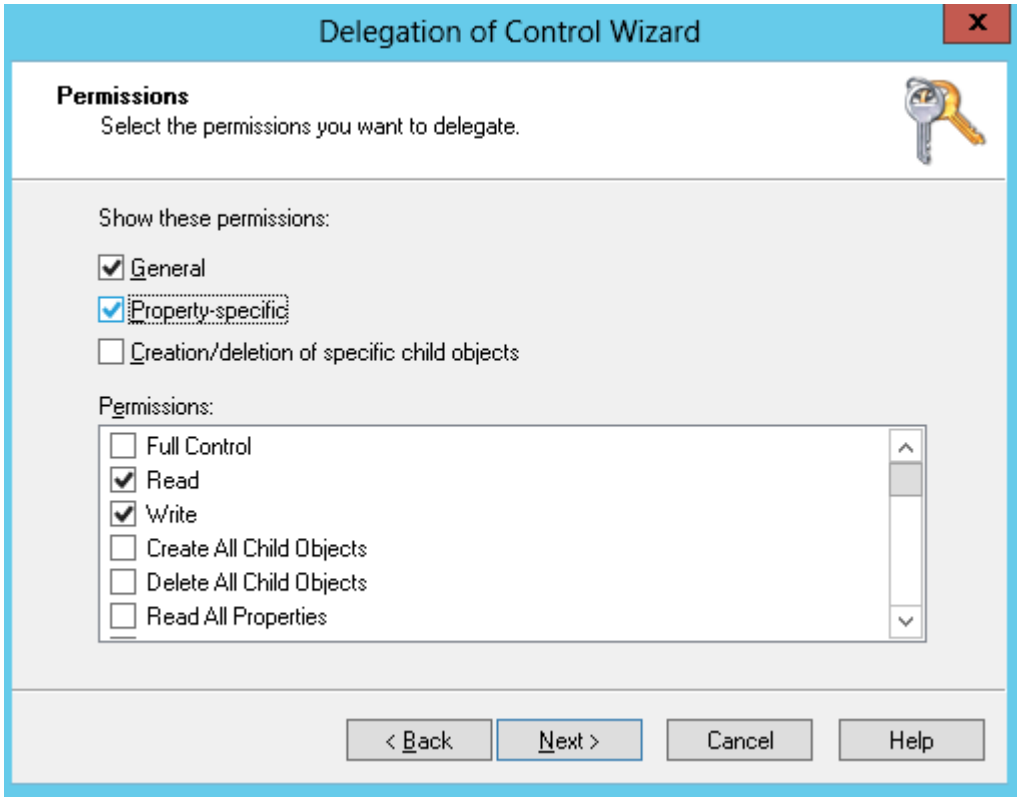
1. Buka Pengguna dan komputer Direktori Aktif dan pilih organizational unit (OU) yang memiliki nama NetBIOS Anda di pohon navigasi, kemudian pilih Pengguna OU.

   > **Important**
   >
   > Saat Anda meluncurkan AWS Directory Service untuk Microsoft Active Directory, AWS buat unit organisasi (OU) yang berisi semua objek direktori Anda. OU ini, yang memiliki nama NetBIOS yang Anda ketik saat membuat direktori Anda, terletak di root domain. Root domain dimiliki dan dikelola oleh AWS. Anda tidak dapat membuat perubahan ke root domain itu sendiri, oleh karena itu, Anda harus membuat grup **`Joiners`** dalam OU yang memiliki nama NetBIOS Anda.

2. Buka menu konteks (klik kanan) untuk Pengguna, pilih Baru, lalu pilih Grup.
3. Di kotak Objek Baru - Grup, ketik hal berikut dan pilih OK.
   - Untuk Nama grup, ketik **`Joiners`**.
   - Untuk Cakupan grup, pilih Global.
   - Untuk Jenis grup, pilih Keamanan.
4. Pada pohon navigasi, pilih kontainer Komputer di bawah nama NetBIOS Anda. Dari menu Tindakan, pilih Kendali Delegasi.
5. Pada halaman Delegasi Control Wizard, pilih Selanjutnya, lalu pilih Tambahkan.
6. Di kotak Pilih Pengguna, Komputer, atau Grup, ketik `Joiners` dan pilih OK. Jika ditemukan lebih dari satu objek, pilih grup `Joiners` yang dibuat di atas. Pilih Berikutnya.
7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Selanjutnya.



10. Pilih Baca dan Tulis, lalu pilih Selanjutnya.



11. Verifikasi informasi pada halaman Menyelesaikan Delegasi Control Wizard, dan klik Selesai.

12. Buat pengguna dengan kata sandi yang kuat dan tambahkan pengguna tersebut ke grup `Joiners`. Pengguna ini harus berada di kontainer Pengguna yang berada di bawah nama NetBIOS Anda. Pengguna tersebut kemudian akan memiliki hak istimewa yang memadai untuk menghubungkan instans ke direktori.

Buat set opsi DHCP

AWS merekomendasikan agar Anda membuat set opsi DHCP untuk AWS Directory Service direktori Anda dan menetapkan opsi DHCP yang disetel ke VPC tempat direktori Anda berada. Ini memungkinkan setiap instans di VPC tersebut mengarah ke domain tertentu, dan server DNS untuk menyelesaikan nama domain mereka.

Untuk informasi selengkapnya tentang set opsi DHCP, lihat Set opsi DHCP di Panduan Pengguna Amazon VPC.

Untuk membuat set opsi DHCP untuk direktori Anda

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Set Opsi DHCP, lalu pilih Buat set opsi DHCP.
3. Pada halaman Buat set opsi DHCP, masukkan nilai berikut untuk direktori Anda:

   Nama

   Tanda opsional untuk set opsi.

   Nama domain

   Nama yang memenuhi syarat untuk direktori, seperti `corp.example.com`.

   Server nama domain

   Alamat IP server DNS direktori AWS-provided Anda.

   > **Note**
   >
   > Anda dapat menemukan alamat ini dengan membuka panel navigasi Konsol AWS Directory Service, memilih direktori dan kemudian memilih ID direktori yang benar.

Server NTP

Biarkan bidang ini kosong.

Server nama NetBIOS

Biarkan bidang ini kosong.

Jenis simpul NetBIOS

Biarkan bidang ini kosong.

4. Pilih Buat set opsi DHCP. Set opsi DHCP baru muncul dalam daftar opsi DHCP Anda.
5. Catat ID dari set opsi DHCP yang baru (dopt-*xxxxxxxx*). Anda menggunakannya untuk mengasosiasikan set opsi yang baru dengan VPC Anda.

Untuk mengubah set opsi DHCP yang terkait dengan VPC

Setelah Anda membuat set opsi DHCP, Anda tidak dapat mengubahnya. Jika Anda ingin VPC Anda untuk menggunakan set opsi DHCP yang berbeda, Anda harus membuat satu set baru dan mengasosiasikannya dengan VPC Anda. Anda juga dapat mengatur VPC Anda untuk tidak menggunakan opsi DHCP sama sekali.

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih VPC Anda
3. Pilih VPC, lalu pilih Tindakan, Edit set opsi DHCP.
4. Untuk Set opsi DHCP, pilih satu set opsi atau pilih Tidak ada set opsi DHCP, lalu pilih Simpan.

Mengelola pengguna dan grup di Microsoft AD yang Dikelola AWS

Pengguna mewakili individu orang atau entitas yang memiliki akses ke direktori Anda. Grup sangat berguna untuk memberikan atau menolak hak istimewa ke grup pengguna, daripada harus menerapkan hak istimewa tersebut ke setiap pengguna. Jika pengguna berpindah ke organisasi yang berbeda, Anda memindahkan pengguna tersebut ke grup yang berbeda dan mereka secara otomatis menerima hak istimewa yang diperlukan untuk organisasi baru.

Untuk membuat pengguna dan grup di direktori AWS Directory Service, Anda harus menggunakan instans apapun (dari on-premise atau EC2) yang telah bergabung ke direktori AWS Directory Service

Anda, dan masuk sebagai pengguna yang memiliki hak istimewa untuk membuat pengguna dan grup. Anda juga perlu menginstal Alat Direktori Aktif pada instans EC2 Anda sehingga Anda dapat menambahkan pengguna dan grup dengan snap-in Pengguna dan Komputer Direktori Aktif.

Anda dapat menerapkan instans EC2 yang telah dikonfigurasi sebelumnya dengan alat administratif Active Directory yang sudah diinstal sebelumnya dari konsol manajemen. AWS Directory Service Untuk informasi selengkapnya, lihat Luncurkan instans administrasi direktori di Microsoft AD AWS Terkelola Active Directory.

Jika Anda perlu menerapkan instans EC2 yang dikelola sendiri dengan alat administratif dan menginstal alat yang diperlukan, lihat. Langkah 3: Menerapkan instans Amazon EC2 untuk mengelola Direktori Aktif Microsoft AD yang AWS Dikelola

> **Note**
>
> Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, tetapi tidak boleh diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka Preauthentication di Microsoft. TechNet

Topik berikut termasuk petunjuk tentang cara membuat dan mengelola pengguna dan grup.

Topik

- Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola
- Buat pengguna
- Hapus pengguna
- Mengatur ulang kata sandi pengguna
- Membuat grup
- Menambahkan pengguna ke grup

Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola

Untuk mengelola Active Directory dari instans Amazon EC2 Windows Server, Anda perlu menginstal Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools pada instans. Gunakan prosedur berikut untuk menginstal alat-alat ini pada instance EC2 Windows Server.

Prasyarat

Sebelum Anda dapat memulai prosedur ini, selesaikan yang berikut ini:

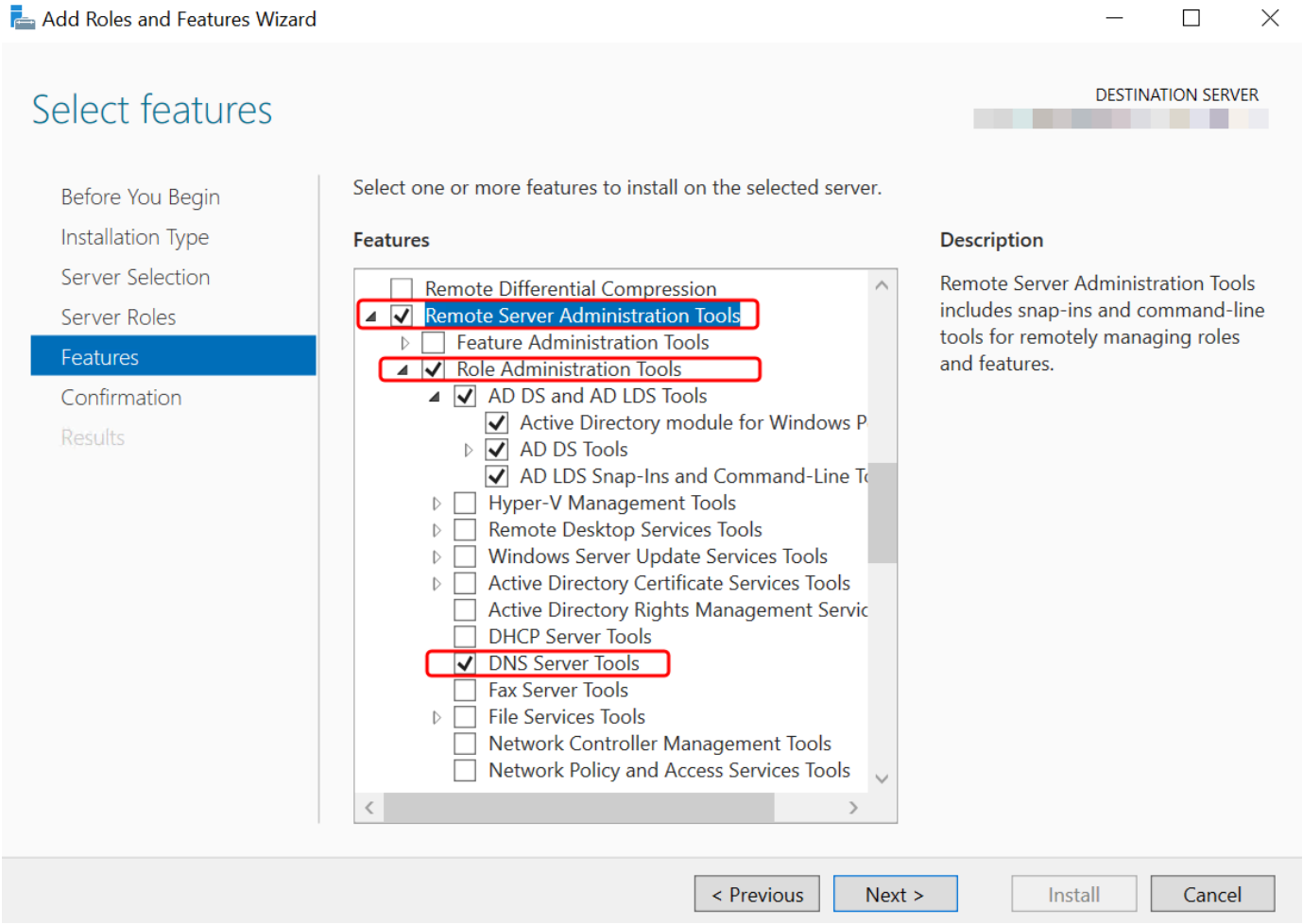
1. Buat Direktori Aktif Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya, lihat Membuat iklan Microsoft AWS Terkelola Active Directory.
2. Luncurkan dan gabungkan instans Windows Server EC2 ke Direktori Aktif Microsoft AD AWS Terkelola Anda. Instans EC2 memerlukan kebijakan berikut untuk membuat pengguna dan grup: **`AWSSSMManagedInstanceCore`** dan**`AmazonSSMDirectoryServiceAccess`**. Lihat informasi yang lebih lengkap di Luncurkan instans administrasi direktori di Microsoft AD AWS Terkelola Active Directory dan Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory.
3. Anda akan memerlukan kredensi untuk Administrator domain Direktori Aktif Anda. Kredensi ini dibuat ketika AD AWS Microsoft yang Dikelola dibuat. Jika Anda mengikuti prosedur diMembuat iklan Microsoft AWS Terkelola Active Directory, nama pengguna Administrator Anda menyertakan nama NetBIOS Anda,. **`corp\admin`**

Instal Alat Administrasi Direktori Aktif pada instans Windows Server EC2

Untuk menginstal alat administrasi Direktori Aktif pada instans EC2 Windows Server

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di konsol Amazon EC2, pilih Instans, pilih instance Windows Server, lalu pilih Connect.
3. Di halaman Connect to instance, pilih klien RDP.
4. Di tab klien RDP, pilih Unduh File Desktop Jarak Jauh, lalu pilih Dapatkan Kata Sandi untuk mengambil kata sandi Anda.
5. Dalam kata sandi Dapatkan Windows, pilih Unggah file kunci pribadi. Pilih file kunci pribadi.pem yang terkait dengan instance Windows Server. Setelah mengunggah file kunci pribadi, pilih Dekripsi kata sandi.
6. Di kotak dialog Keamanan Windows, salin kredensi administrator lokal Anda untuk komputer Windows Server untuk masuk. Nama pengguna dapat dalam format berikut: ***`NetBIOS-Name`*`\admin`** atau***`DNS-Name`*`\admin`**. Misalnya, **`corp\admin`** akan menjadi nama pengguna jika Anda mengikuti prosedur diMembuat iklan Microsoft AWS Terkelola Active Directory.
7. Setelah masuk ke instance Windows Server, buka Server Manager dari menu Start dengan memilih Server Manager.
8. Di Dasbor Manajer Server, pilih Tambahkan peran dan fitur.

9. Di Tambahkan peran dan fitur Wizard pilih Jenis Instalasi, pilih Instalasi berbasis peran atau berbasis fitur, dan pilih Selanjutnya.
10. Di bawah Pilihan Server, pastikan server lokal dipilih, dan pilih Fitur di panel navigasi sebelah kiri.
11. Di pohon Fitur, pilih dan buka Alat Administrasi Server Jarak Jauh, Alat Administrasi Peran, dan Alat AD DS dan AD LDS. Dengan AD DS dan AD LDS Tools dipilih, Active Directorymodul untuk, AD DS ToolsWindows PowerShell, dan AD LDS Snap-in dan Command-Line Tools dipilih. Gulir ke bawah dan pilih DNS Server Tools, lalu pilih Berikutnya.



12. Tinjau informasi dan pilih Instal. Ketika instalasi fitur selesai, Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools tersedia dari menu Start di folder Administrative Tools.

Metode Alternatif untuk menginstal Alat Administrasi Direktori Aktif pada instans Server Windows EC2

- Berikut adalah beberapa metode lain untuk menginstal Alat Administrasi Direktori Aktif:
  - Anda dapat memilih untuk menginstal Alat Administrasi Direktori Aktif menggunakanWindows PowerShell. Misalnya, Anda dapat menginstal alat administrasi jarak jauh Active Directory dari PowerShell prompt menggunakan`Install-WindowsFeature RSAT-ADDS`. Untuk informasi selengkapnya, lihat Menginstal- WindowsFeature di situs web Microsoft.
  - Anda juga dapat meluncurkan instans EC2 administrasi direktori AWS Management Console yang sudah memiliki Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools diinstal dengan mengikuti prosedur diLuncurkan instans administrasi direktori di Microsoft AD AWS Terkelola Active Directory.

Buat pengguna

Gunakan prosedur berikut untuk membuat pengguna dengan instans EC2 yang digabungkan ke direktori Microsoft AD yang Dikelola AWS Anda. Sebelum Anda dapat membuat pengguna, Anda harus menyelesaikan prosedur di Instalasi Alat Administrasi Direktori Aktif.

Anda dapat menggunakan salah satu metode berikut untuk membuat pengguna:

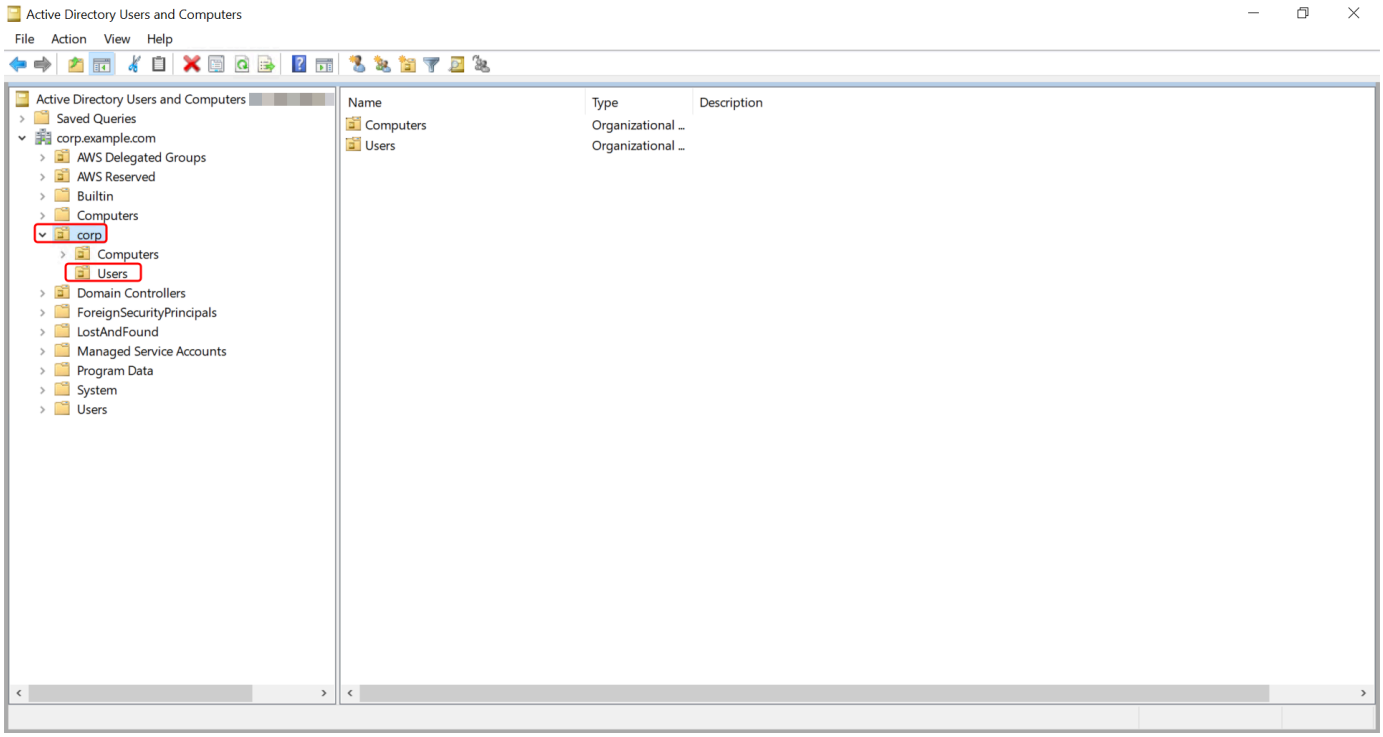
- Active DirectoryAlat Administrasi
- Windows PowerShell

Buat pengguna dengan Alat Active Directory Administrasi

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Active Directory Users and Computers dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

> **Tip**
>
> Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Di pohon direktori, pilih OU di bawah nama NetBIOS direktori Anda OU di mana Anda ingin menyimpan pengguna Anda (misalnya,**`corp\Users`**). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihatApa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.



4. Pada menu Tindakan, pilih Baru, lalu pilih Pengguna untuk membuka wizard pengguna baru.
5. Pada halaman pertama wizard, masukkan nilai untuk bidang berikut, lalu pilih Berikutnya.
   - Nama depan
   - Nama belakang
   - Nama logon pengguna
6. Pada halaman kedua wizard, masukkan kata sandi sementara di Kata Sandi dan Konfirmasi Kata Sandi. Pastikan pilihan Pengguna harus mengubah kata sandi pada proses masuk berikutnya dipilih. Tidak satu pun dari pilihan lain harus dipilih. Pilih Berikutnya.
7. Pada halaman ketiga wizard, verifikasi bahwa informasi pengguna baru sudah benar dan pilih Selesai. Pengguna baru akan muncul di folder Pengguna.

Buat pengguna di Windows PowerShell

1. Connect ke instance yang bergabung dengan Active Directory domain Anda sebagai Active Directory administrator.

2. Buka Windows PowerShell.
3. Ketik perintah berikut mengganti nama pengguna **`jane.doe`** dengan nama pengguna pengguna yang ingin Anda buat. Anda akan diminta Windows PowerShell untuk memberikan kata sandi untuk pengguna baru. Untuk informasi selengkapnya tentang persyaratan kompleksitas Active Directory kata sandi, lihat Microsoftdokumentasi. Untuk informasi selengkapnya tentang perintah New-aduser, lihat dokumentasi. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Hapus pengguna

Gunakan prosedur berikut untuk menghapus pengguna yang bergabung dengan iklan Microsoft AWS Terkelola AndaActive Directory.

Anda dapat menggunakan salah satu metode berikut untuk menghapus pengguna:

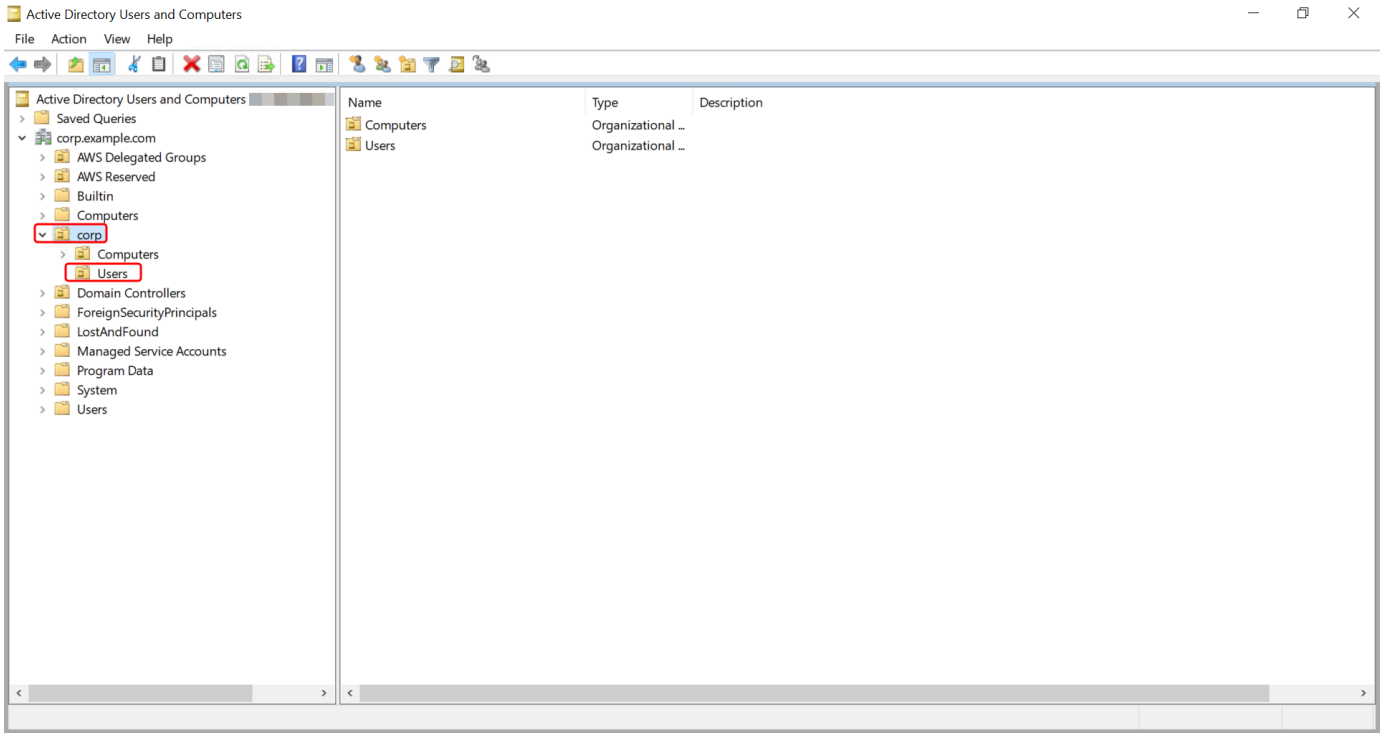
- Active DirectoryAlat Administrasi
- Windows PowerShell

Hapus pengguna dengan Alat Active Directory Administrasi

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

   > **Tip**
   >
   > Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Di pohon direktori, pilih OU yang berisi pengguna yang ingin Anda hapus (misalnya,**`corp\Users`**).



4. Pilih pengguna yang ingin Anda hapus. Pada menu Tindakan, pilih Hapus.
5. Kotak dialog akan muncul meminta Anda untuk mengonfirmasi bahwa Anda ingin menghapus pengguna. Pilih Ya untuk menghapus pengguna. Ini menghapus pengguna yang dipilih secara permanen.

Hapus pengguna di Windows PowerShell

1. Connect ke instance yang bergabung dengan Active Directory domain Anda sebagai Active Directory administrator.
2. Buka Windows PowerShell.
3. Ketik perintah berikut mengganti nama pengguna **`jane.doe`** dengan nama pengguna pengguna yang ingin Anda hapus. Untuk informasi selengkapnya tentang perintah Remove-aduser, lihat dokumentasi. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Pertimbangan Tempat Sampah AD

Pengguna yang dihapus disimpan sementara di Tempat Sampah AD. Untuk informasi selengkapnya tentang Tempat Sampah AD, lihat Tempat Sampah AD Recycle: Memahami, Menerapkan, Praktik Terbaik, dan Pemecahan Masalah di blog Ask the Directory Microsoft Services Team.

Mengatur ulang kata sandi pengguna

Pengguna harus mematuhi kebijakan kata sandi sebagaimana didefinisikan dalamActive Directory. Terkadang ini bisa mendapatkan yang terbaik dari pengguna, termasuk Active Directory administrator, dan mereka lupa kata sandi mereka. Ketika ini terjadi, Anda dapat dengan cepat mengatur ulang kata sandi pengguna menggunakan AWS Directory Service jika pengguna berada di Microsoft AD yang AWS Dikelola.

Anda harus masuk sebagai pengguna dengan izin yang diperlukan untuk mengatur ulang kata sandi. Untuk informasi selengkapnya tentang izin, lihat Ikhtisar mengelola izin akses ke sumber daya Anda AWS Directory Service.

Anda dapat mengatur ulang kata sandi untuk setiap pengguna di Anda Active Directory dengan pengecualian berikut:

- Anda dapat mengatur ulang kata sandi untuk setiap pengguna dalam Unit Organisasi (OU) yang didasarkan dari nama NetBIOS yang Anda gunakan saat Anda membuat. Active Directory Misalnya, jika Anda mengikuti prosedur dalam nama NetBIOS Membuat iklan Microsoft AWS Terkelola Active Directory Anda akan menjadi CORP dan kata sandi pengguna yang dapat Anda atur ulang akan menjadi anggota Corp/Users OU.
- Anda tidak dapat mengatur ulang kata sandi pengguna mana pun di luar OU yang didasarkan pada nama NetBIOS yang Anda gunakan saat Anda membuat. Active Directory Misalnya, Anda tidak dapat mengatur ulang kata sandi untuk pengguna di OU AWS Cadangan. Untuk informasi selengkapnya tentang struktur OU untuk Microsoft AD yang AWS Dikelola, lihatApa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.

Untuk informasi selengkapnya tentang cara kebijakan kata sandi diterapkan saat kata sandi disetel ulang di Microsoft AD yang AWS Dikelola, lihatBagaimana kebijakan kata sandi diterapkan.

Anda dapat menggunakan salah satu metode berikut untuk mengatur ulang kata sandi pengguna:

- AWS Management Console

- AWS CLI
- Windows PowerShell

Setel ulang kata sandi pengguna di AWS Management Console

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori, lalu pilih Active Directory dalam daftar tempat Anda ingin mengatur ulang kata sandi pengguna.
2. Pada halaman Detail direktori, pilih Tindakan, lalu pilih Setel ulang kata sandi pengguna.
3. Dalam dialog Reset kata sandi pengguna, di Nama pengguna ketikkan nama pengguna pengguna yang kata sandinya perlu diubah.
4. Ketik kata sandi di Kata sandi baru dan Konfirmasi kata sandi, lalu pilih Atur ulang sandi.

Setel ulang kata sandi pengguna di AWS CLI

1. Untuk menginstal AWS CLI, lihat Menginstal atau memperbarui versi terbaru dari file AWS CLI.
2. Buka AWS CLI.
3. Ketik perintah berikut dan ganti ID Direktori, nama pengguna**jane.doe**, dan kata sandi **P@ssw0rd** dengan ID Active Directory Direktori Anda dan kredensi yang diinginkan. Lihat reset-user-passworddi Referensi AWS CLI Perintah untuk informasi lebih lanjut.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Setel ulang kata sandi pengguna di Windows PowerShell

1. Connect ke instance yang bergabung dengan Active Directory domain Anda sebagai Active Directory administrator.
2. Buka Windows PowerShell.
3. Ketik perintah berikut mengganti nama pengguna**jane.doe**, ID Direktori, dan kata sandi **P@ssw0rd** dengan ID Active Directory Direktori Anda dan kredensi yang diinginkan. Lihat Reset-DS UserPassword Cmdlet untuk informasi selengkapnya.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Membuat grup

Gunakan prosedur berikut untuk membuat grup keamanan dengan instans EC2 yang bergabung dengan direktori Microsoft AD AWS Terkelola Anda. Sebelum Anda dapat membuat grup keamanan, Anda harus menyelesaikan prosedur di Menginstal Alat Administrasi Direktori Aktif.

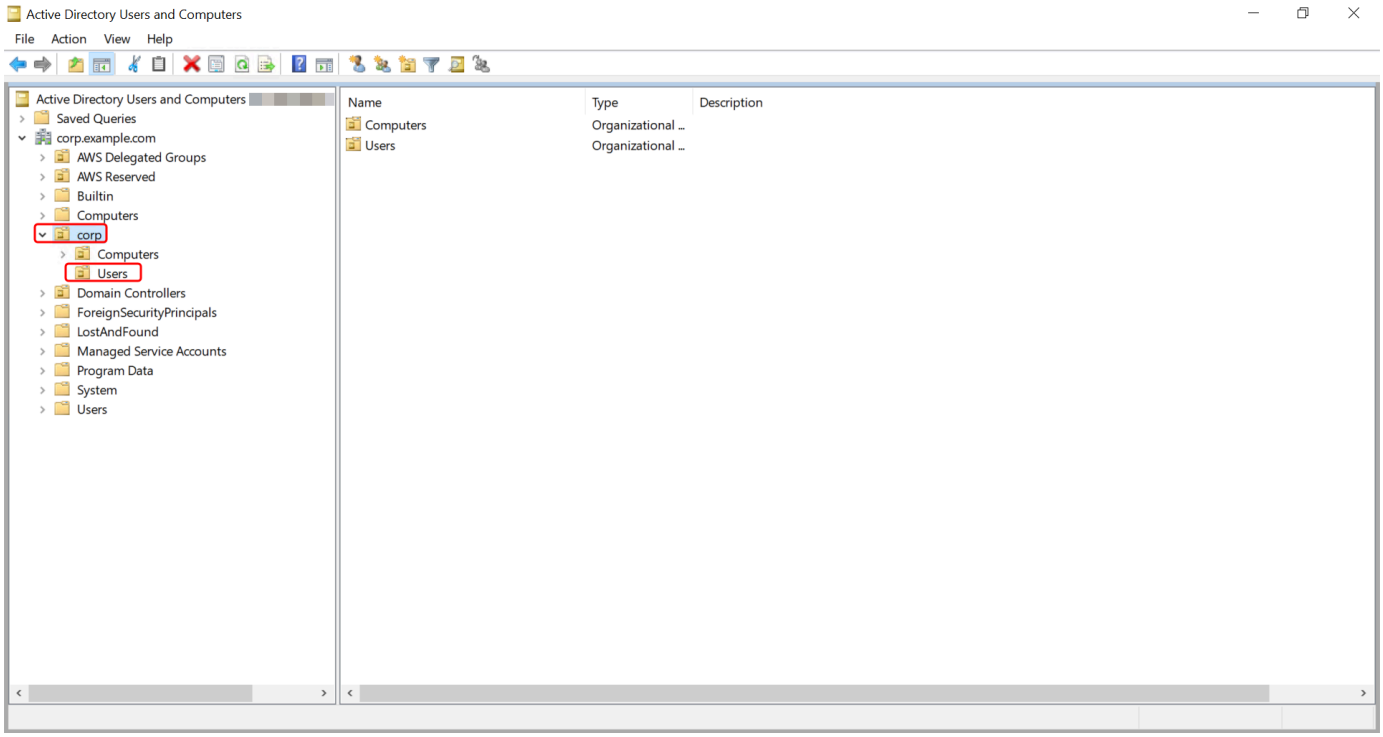
Anda juga dapat menggunakan Windows PowerShell perintah untuk membuat grup. Untuk informasi selengkapnya, lihat New-AdGroup di dokumentasi Windows Server 2022. PowerShell

Untuk membuat grup

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

   > **Tip**
   >
   > Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Pada pohon direktori, pilih OU di bawah direktori OU nama NetBIOS Anda di mana Anda ingin menyimpan grup Anda (misalnya, Corp\Users). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihatApa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.



4. Pada menu Tindakan, klik Baru, dan kemudian klik Grup untuk membuka wizard grup baru.
5. Ketik nama untuk grup di Nama grup, pilih lingkup Grup yang memenuhi kebutuhan Anda, dan pilih Keamanan untuk jenis Grup. Untuk informasi selengkapnya tentang cakupan grup Active Directory dan grup keamanan, lihat Grup keamanan Active Directory di dokumentasi Microsoft Windows Server.
6. Klik OK. Grup keamanan baru akan muncul di folder Pengguna.

Menambahkan pengguna ke grup

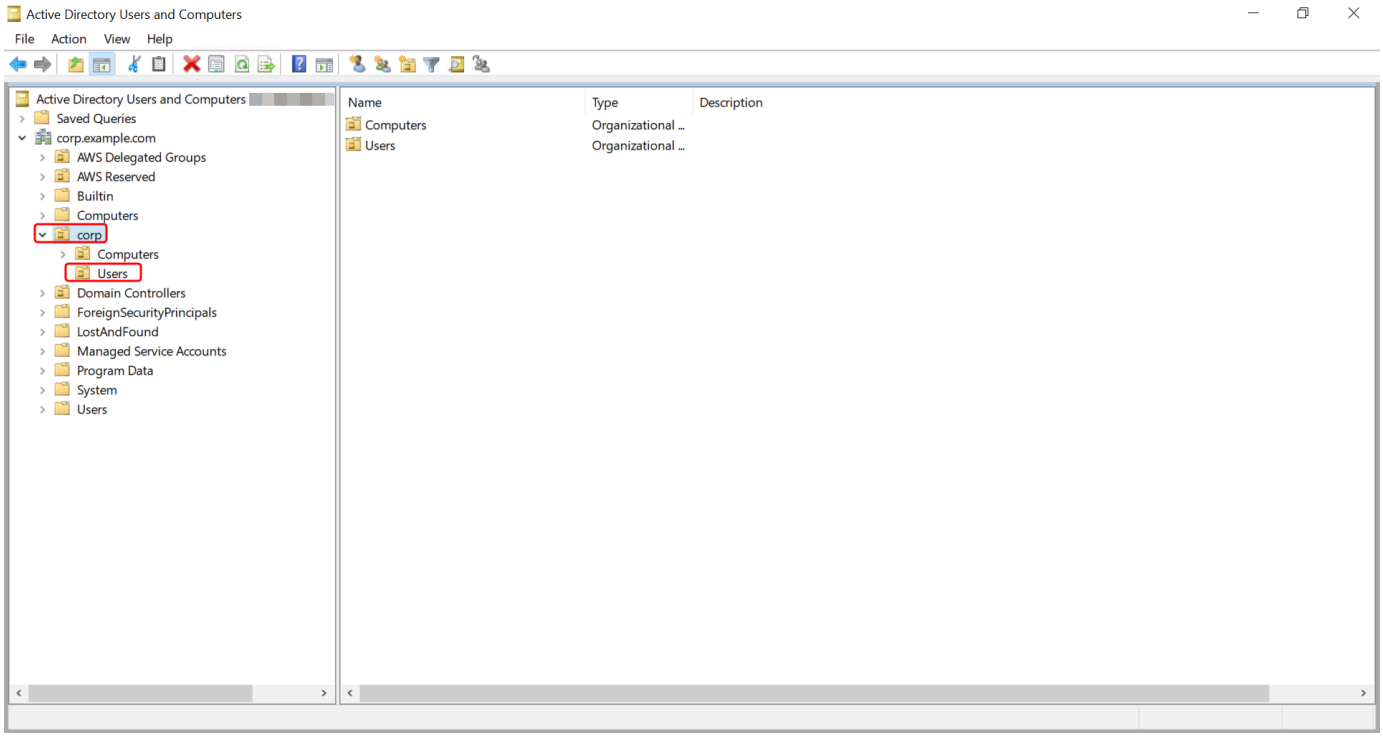
Gunakan prosedur berikut untuk menambahkan pengguna ke grup keamanan dengan instans EC2 yang digabungkan ke direktori Microsoft AD yang Dikelola AWS Anda.

Untuk menambahkan pengguna ke grup

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

> **Tip**
>
> Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Pada pohon direktori, pilih OU di bawah direktori Anda NetBIOS nama OU di mana Anda disimpan grup Anda, dan pilih grup yang Anda ingin tambahkan pengguna sebagai anggota.



4. Pada menu Tindakan, klik Properti untuk membuka kotak dialog properti untuk grup.
5. Pilih tab Anggota dan klik Tambahkan.
6. Untuk Masukkan nama objek yang akan dipilih, ketik nama pengguna yang ingin Anda tambahkan dan klik OK. Nama akan ditampilkan dalam daftar Anggota. Klik OK lagi untuk memperbarui keanggotaan grup.
7. Verifikasikan bahwa pengguna tersebut sekarang adalah anggota grup dengan memilih pengguna di folder Pengguna dan klik Properti di menu Tindakan untuk membuka kotak dialog properti. Pilih tab Anggota dari. Anda harus melihat nama grup dalam daftar grup yang dimiliki pengguna.

Connect ke infrastruktur Active Directory yang ada

Bagian ini menjelaskan cara mengonfigurasi hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan infrastruktur Direktori Aktif yang ada.

Topik

- Menciptakan hubungan kepercayaan
- Menambahkan rute IP saat menggunakan alamat IP publik
- Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri
- Tutorial: Membuat hubungan kepercayaan antara duaAWSDomain Microsoft AD yang Dikelola

Menciptakan hubungan kepercayaan

Anda dapat mengonfigurasi hubungan kepercayaan eksternal dan hutan satu dan dua arah antara AWS Directory Service for Microsoft Active Directory dan direktori yang dikelola sendiri (lokal), serta di antara beberapa direktori AWS Microsoft AD Terkelola di cloud. AWS AWS Microsoft AD yang dikelola mendukung ketiga arah hubungan kepercayaan: Masuk, Keluar, dan Dua arah (Bi-directional).

Untuk informasi selengkapnya tentang hubungan kepercayaan, lihat Semua yang ingin Anda ketahui tentang kepercayaan dengan Microsoft AD yang AWS Dikelola.

> **Note**
>
> Saat mengatur hubungan kepercayaan, Anda harus memastikan bahwa direktori yang dikelola sendiri dan tetap kompatibel dengan AWS Directory Service s. Untuk informasi selengkapnya tentang tanggung jawab Anda, silakan lihat model tanggung jawab bersama kami.

AWS Microsoft AD yang dikelola mendukung perwalian eksternal dan hutan. Untuk menelusuri contoh skenario yang menunjukkan cara membuat kepercayaan forest, lihat Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri.

Kepercayaan dua arah diperlukan untuk Aplikasi AWS Perusahaan seperti Amazon Chime, Amazon Connect, Amazon,, QuickSight Amazon AWS IAM Identity Center, Amazon WorkDocs, Amazon

WorkMail, WorkSpaces Amazon, dan. AWS Management Console AWS Microsoft AD yang dikelola harus dapat menanyakan pengguna dan grup yang dikelola sendiriActive Directory.

Amazon EC2, Amazon RDS, dan Amazon FSx akan bekerja dengan kepercayaan satu arah atau dua arah.

Prasyarat

Membuat kepercayaan hanya memerlukan beberapa langkah, tetapi Anda harus terlebih dahulu menyelesaikan beberapa langkah prasyarat sebelum mengatur kepercayaan.

> **Note**
>
> AWS Microsoft AD yang dikelola tidak mendukung kepercayaan dengan Domain Label Tunggal.

Menghubungkan ke VPC

Jika Anda membuat hubungan kepercayaan dengan direktori yang dikelola sendiri, Anda harus terlebih dahulu menghubungkan jaringan yang dikelola sendiri ke VPC Amazon yang berisi iklan Microsoft yang Dikelola AWS . Firewall untuk jaringan Microsoft AD yang AWS dikelola sendiri dan dikelola harus membuka port jaringan yang terdaftar di WindowsServer 2008 dan versi yang lebih baru dalam Microsoft dokumentasi.

Untuk menggunakan nama NetBIOS Anda alih-alih nama domain lengkap Anda untuk otentikasi dengan aplikasi Anda AWS seperti Amazon WorkDocs atau QuickSight Amazon, Anda harus mengizinkan port 9389. Untuk informasi selengkapnya tentang port dan protokol Direktori Aktif, lihat Ringkasan layanan dan persyaratan port jaringan untuk dokumentasi Windows. Microsoft

Ini adalah port-port minimum yang diperlukan untuk dapat terhubung ke direktori Anda. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Mengkonfigurasi VPC Anda

VPC yang berisi iklan AWS Microsoft Terkelola Anda harus memiliki aturan keluar dan masuk yang sesuai.

Untuk mengkonfigurasi aturan keluar VPC Anda

1. Di AWS Directory Service konsol, pada halaman Detail Direktori, catat ID direktori Microsoft AD AWS Terkelola Anda.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Pilih Grup Keamanan.
4. Cari ID direktori Microsoft AD AWS Terkelola Anda. Dalam hasil pencarian, pilih item dengan deskripsi "AWS membuat grup keamanan untuk pengontrol direktori ID direktori".

   > **Note**
   >
   > Grup keamanan yang dipilih adalah grup keamanan yang dibuat secara otomatis ketika Anda awalnya membuat direktori Anda.

5. Pergi ke tab Aturan Keluar dari grup keamanan tersebut. Pilih Edit, kemudian Tambahkan aturan lain. Untuk aturan baru, masukkan nilai berikut:

   - Jenis: Semua Lalu lintas
   - Protokol: Semua
   - Tujuan menentukan lalu lintas yang dapat meninggalkan pengontrol domain Anda dan ke mana ia dapat pergi di jaringan yang dikelola sendiri. Tentukan alamat IP tunggal atau cakupan alamat IP dalam notasi CIDR (misalnya, 203.0.113.5/32). Anda juga dapat menentukan nama atau ID grup keamanan lain di Region yang sama. Untuk informasi selengkapnya, lihat Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan.

6. Pilih Simpan.

Aktifkan pra-autentikasi Kerberos

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Untuk informasi selengkapnya tentang setelan ini, tinjau Pra-otentikasi di Microsoft. TechNet

Konfigurasikan forwarder bersyarat DNS pada domain yang dikelola sendiri

Anda harus menyiapkan forwarder bersyarat DNS pada domain yang dikelola sendiri. Lihat Menetapkan Forwarder Bersyarat untuk Nama Domain di Microsoft TechNet untuk detail tentang penerusan bersyarat.

Untuk melakukan langkah-langkah berikut, Anda harus memiliki akses ke alat Windows Server berikut untuk domain yang dikelola sendiri:

- Alat AD DS dan AD LDS
- DNS

Untuk mengonfigurasi forwarder bersyarat pada domain yang dikelola sendiri

1. Pertama, Anda harus mendapatkan beberapa informasi tentang Microsoft AD yang AWS Dikelola. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Di panel navigasi , pilih Direktori.
3. Pilih ID direktori iklan Microsoft AWS Terkelola Anda.
4. Perhatikan nama domain yang memenuhi syarat (FQDN) dan alamat DNS dari direktori Anda.
5. Sekarang, kembali ke pengontrol domain yang dikelola sendiri. Buka Pengelola Server
6. Pada menu Alat, pilih DNS.
7. Pada pohon konsol, perluas server DNS dari domain di mana Anda mengatur kepercayaan.
8. Pada pohon konsol, pilih Penerusan Bersyarat.
9. Pada menu Tindakan, pilih Penerusan bersyarat baru.
10. Di domain DNS, ketik nama domain yang memenuhi syarat penuh (FQDN) dari AWS Microsoft AD Terkelola Anda, yang Anda sebutkan sebelumnya.
11. Pilih alamat IP server master dan ketik alamat DNS direktori Microsoft AD AWS Terkelola Anda, yang Anda catat sebelumnya.

    Setelah memasukkan alamat DNS, Anda mungkin mendapatkan error “timeout” atau “tidak dapat menyelesaikan”. Anda biasanya dapat mengabaikan error ini.
12. Pilih Menyimpan penerusan bersyarat ini di Direktori Aktif dan mereplikasi sebagai berikut: Semua server DNS di domain ini. Pilih OK.

Kata sandi hubungan Kepercayaan

Jika Anda membuat hubungan kepercayaan dengan domain yang ada, atur hubungan kepercayaan pada domain tersebut menggunakan alat Administrasi Server Windows. Saat Anda melakukannya, perhatikan kata sandi kepercayaan yang Anda gunakan. Anda harus menggunakan kata sandi yang sama ini saat mengatur hubungan kepercayaan pada iklan Microsoft yang AWS Dikelola. Untuk informasi selengkapnya, lihat Mengelola Trust di Microsoft TechNet.

Anda sekarang siap untuk menciptakan hubungan kepercayaan pada iklan Microsoft yang AWS Dikelola.

NetBIOS dan Nama Domain

NetBIOS dan nama domain harus unik dan tidak bisa sama untuk membangun hubungan kepercayaan.

Membuat, memverifikasi, atau menghapus hubungan kepercayaan

> **Note**
>
> Hubungan kepercayaan adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus dilakukan di Region primer. Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk membuat hubungan kepercayaan dengan Microsoft AD yang AWS Dikelola

1. Buka konsol AWS Directory Service.
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Pada halaman Tambahkan hubungan kepercayaan, berikan informasi yang diperlukan, termasuk jenis kepercayaan, fully qualified domain name (FQDN) dari domain tepercaya Anda, kata sandi kepercayaan dan arah kepercayaan.
6. (Opsional) Jika Anda hanya ingin mengizinkan pengguna yang berwenang untuk mengakses sumber daya di direktori Microsoft AD AWS Terkelola, Anda dapat memilih kotak centang Autentikasi selektif secara opsional. Untuk informasi umum tentang otentikasi selektif, lihat Pertimbangan Keamanan untuk Trusts di Microsoft. TechNet

7. Untuk Conditional forwarder, ketikkan alamat IP server DNS yang dikelola sendiri. Jika sebelumnya Anda telah membuat kondisional forwarder, Anda dapat mengetik FQDN dari domain yang dikelola sendiri alih-alih alamat IP DNS.
8. (Opsional) Pilih Tambahkan alamat IP lain dan ketik alamat IP server DNS tambahan yang dikelola sendiri. Anda dapat mengulangi langkah ini untuk setiap alamat server DNS yang berlaku untuk total empat alamat.
9. Pilih Tambahkan.
10. Jika server DNS atau jaringan untuk domain yang dikelola sendiri menggunakan ruang alamat IP publik (non-RFC 1918), buka bagian perutean IP, pilih Tindakan, lalu pilih Tambahkan rute. Ketik blok alamat IP server DNS Anda atau jaringan yang dikelola sendiri menggunakan format CIDR, misalnya 203.0.113.0/24. Langkah ini tidak diperlukan jika server DNS Anda dan jaringan yang dikelola sendiri menggunakan ruang alamat IP RFC 1918.

    > **Note**
    >
    > Saat menggunakan ruang alamat IP publik, pastikan bahwa Anda tidak menggunakan salah satu dari Rentang alamat IP AWS karena ini tidak dapat digunakan.

11. (Opsional) Kami merekomendasikan bahwa saat Anda berada di halaman Tambahkan rute Anda juga pilih Menambahkan rute ke grup keamanan untuk VPC direktori ini. Ini akan mengkonfigurasi grup keamanan seperti yang dijelaskan di atas dalam “Konfigurasi VPC Anda.” Aturan keamanan ini memengaruhi antarmuka jaringan internal yang tidak terbuka secara publik. Jika opsi ini tidak tersedia, Anda akan melihat pesan yang menunjukkan bahwa Anda telah menyesuaikan grup keamanan Anda.

Anda harus mengatur hubungan kepercayaan pada kedua domain. Hubungan harus saling melengkapi. Misalnya, jika Anda membuat kepercayaan keluar pada satu domain, Anda harus membuat kepercayaan masuk di sisi lain.

Jika Anda membuat hubungan kepercayaan dengan domain yang ada, atur hubungan kepercayaan pada domain tersebut menggunakan alat Administrasi Server Windows.

Anda dapat membuat beberapa kepercayaan antara Microsoft AD yang AWS Dikelola dan berbagai domain Direktori Aktif. Namun, hanya satu hubungan kepercayaan per pasangan dapat eksis pada suatu waktu. Misalnya, jika Anda memiliki kepercayaan satu arah yang ada di “Arah masuk” dan Anda kemudian ingin mengatur hubungan kepercayaan lain di “Arah keluar,” Anda perlu menghapus hubungan kepercayaan yang ada, dan membuat kepercayaan “Dua arah” baru.

Untuk memverifikasi hubungan kepercayaan keluar

1. Buka konsol AWS Directory Service.
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih kepercayaan yang ingin Anda verifikasi, pilih Tindakan, dan kemudian pilih Verifikasi hubungan kepercayaan.

Proses ini hanya memverifikasi arah keluar dari kepercayaan dua arah. AWS tidak mendukung verifikasi perwalian yang masuk. Untuk informasi selengkapnya tentang cara memverifikasi kepercayaan ke atau dari Direktori Aktif yang dikelola sendiri, lihat Verifikasi Kepercayaan di Microsoft TechNet.

Untuk menghapus hubungan kepercayaan yang ada

1. Buka konsol AWS Directory Service.
2. Pada halaman Direktori, pilih ID AD Microsoft yang AWS Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih kepercayaan yang ingin Anda hapus, pilih Tindakan, dan kemudian pilih Hapus hubungan kepercayaan.
5. Pilih Hapus.

Menambahkan rute IP saat menggunakan alamat IP publik

Anda dapat menggunakan Directory Service AWS untuk Microsoft Active Directory untuk mengambil keuntungan dari banyak fitur Active Directory yang kuat, termasuk membangun kepercayaan dengan direktori lain. Namun, jika server DNS untuk jaringan direktori lain menggunakan alamat IP publik (non-RFC 1918), Anda harus menentukan alamat IP tersebut sebagai bagian dari konfigurasi kepercayaan. Petunjuk untuk melakukan ini dapat ditemukan di Menciptakan hubungan kepercayaan.

Demikian pula, Anda juga harus memasukkan informasi alamat IP saat merutekan lalu lintas dari Microsoft AD yang Dikelola AWS Anda pada AWS ke VPC AWS peer, jika VPC menggunakan rentang IP publik.

Saat Anda menambahkan alamat IP seperti yang dijelaskan di Menciptakan hubungan kepercayaan, Anda memiliki pilihan untuk memilih Menambahkan rute ke grup keamanan untuk VPC direktori ini. Opsi ini harus dipilih kecuali Anda sebelumnya telah menyesuaikan Grup keamanan Anda untuk memungkinkan lalu lintas yang diperlukan seperti yang ditunjukkan di bawah. Untuk informasi selengkapnya, lihat Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan.

Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri

Tutorial ini memandu Anda melalui semua langkah yang diperlukan untuk mengatur hubungan kepercayaan antara AWS Directory Service untuk Microsoft Active Directory dan Microsoft Active Directory yang dikelola sendiri (lokal). Meskipun membuat kepercayaan hanya memerlukan beberapa langkah, Anda harus terlebih dahulu menyelesaikan langkah-langkah prasyarat berikut.

Topik

- Prasyarat
- Langkah 1: Siapkan Domain AD yang dikelola sendiri
- Langkah 2: Siapkan Microsoft AD yang Dikelola AWS
- Langkah 3: Buat hubungan kepercayaan

Lihat juga

Menciptakan hubungan kepercayaan

Prasyarat

Tutorial ini mengasumsikan bahwa Anda telah memiliki hal berikut:

> **Note**
>
> Microsoft AD yang Dikelola AWS tidak mendukung kepercayaan dengan Domain Label Tunggal.

- Direktori Microsoft AD yang Dikelola AWS dibuat di AWS. Jika Anda memerlukan bantuan untuk melakukannya, lihat Memulai dengan Microsoft AD yang AWS Dikelola.
- Instans EC2 yang menjalankan Windows ditambahkan ke Microsoft AD yang Dikelola AWS tersebut. Jika Anda memerlukan bantuan untuk melakukannya, lihat Menggabungkan instans Windows Amazon EC2 secara manual ke Direktori Aktif AWS Microsoft AD Terkelola.

  > **Important**
  >
  > Akun admin untuk Microsoft AD yang Dikelola AWS harus memiliki akses administratif ke instans ini.

- Alat Windows Server berikut diinstal pada instans tersebut:
  - Alat AD DS dan AD LDS
  - DNS

  Jika Anda memerlukan bantuan untuk melakukannya, lihat Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola.
- Microsoft Active Directory yang dikelola sendiri (lokal)

  Anda harus memiliki akses administratif ke direktori ini. Alat Windows Server yang sama seperti yang tercantum di atas juga harus tersedia untuk direktori ini.
- Sambungan aktif antara jaringan yang dikelola sendiri dan VPC yang berisi iklan Microsoft AWS Terkelola Anda. Jika Anda memerlukan bantuan untuk melakukannya, lihat Pilihan Konektivitas Amazon Virtual Private Cloud.
- Kebijakan keamanan lokal yang ditetapkan dengan benar. Periksa `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` dan pastikan bahwa itu berisi setidaknya tiga pipa bernama berikut:
  - netlogon
  - samr
  - lsarpc

- NetBIOS dan nama domain harus unik dan tidak bisa sama untuk membangun hubungan kepercayaan

Untuk informasi lebih lanjut tentang prasyarat untuk menciptakan hubungan kepercayaan, lihat. Menciptakan hubungan kepercayaan

Konfigurasi tutorial

Untuk tutorial ini, kami telah membuat iklan Microsoft yang AWS Dikelola dan domain yang dikelola sendiri. Jaringan yang dikelola sendiri terhubung ke VPC Microsoft AD yang AWS Dikelola. Berikut ini adalah properti dari dua direktori tersebut:

Microsoft AD yang Dikelola AWS berjalan pada AWS

- Nama domain (FQDN): Ad.example.com MyManaged
- Nama NetBIOS: AD MyManaged
- Alamat DNS: 10.0.10.246, 10.0.20.121
- VPC CIDR: 10.0.0.0/16

Microsoft AD yang Dikelola AWS berada di ID VPC: vpc-12345678.

Domain Microsoft AD yang AWS dikelola sendiri atau Dikelola

- Nama domain (FQDN): corp.example.com
- Nama NetBIOS: CORP
- Alamat DNS: 172.16.10.153
- CIDR yang dikelola sendiri: 172.16.0.0/16

Langkah selanjutnya

Langkah 1: Siapkan Domain AD yang dikelola sendiri

Langkah 1: Siapkan Domain AD yang dikelola sendiri

Pertama, Anda perlu menyelesaikan beberapa langkah prasyarat pada domain yang dikelola sendiri (lokal) Anda.

Konfigurasikan firewall yang dikelola sendiri

Anda harus mengonfigurasi firewall yang dikelola sendiri sehingga port berikut terbuka ke CIDR untuk semua subnet yang digunakan oleh VPC yang berisi iklan Microsoft Terkelola Anda. AWS Dalam tutorial ini, kami mengizinkan lalu lintas masuk dan keluar dari 10.0.0.0/16 (blok CIDR dari VPC AWS Microsoft AD Terkelola kami) pada port berikut:

- TCP/UDP 53 - Sistem Nama Domain (DNS)
- TCP/UDP 88 - Autentikasi Kerberos
- TCP/UDP 389 - Protokol Akses Direktori Ringan (LDAP)
- TCP 445 - Blok Pesan Server (SMB)
- TCP 9389 - Layanan Web Direktori Aktif (ADWS) (Opsional - Port ini harus terbuka jika Anda ingin menggunakan nama NetBIOS Anda alih-alih nama domain lengkap Anda untuk otentikasi dengan aplikasi seperti AWS Amazon atau Amazon.) WorkDocs QuickSight

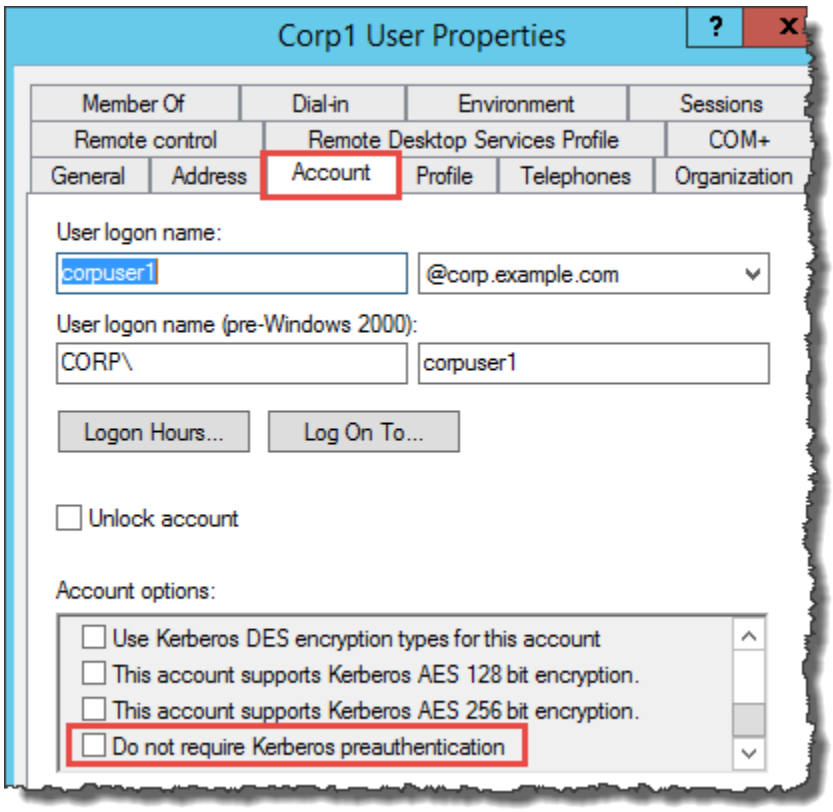
> **Note**
>
> SMBv1 tidak lagi didukung.
> Ini adalah port minimum yang diperlukan untuk menghubungkan VPC ke direktori yang dikelola sendiri. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Pastikan bahwa Kerberos pra-autentikasi diaktifkan

Akun pengguna di kedua direktori harus mengaktifkan praautentikasi Kerberos. Ini adalah default, tapi mari kita periksa properti dari setiap pengguna acak untuk memastikan tidak ada yang berubah.

Untuk melihat setelan Kerberos pengguna

1. Pada pengontrol domain yang dikelola sendiri, buka Server Manager.
2. Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
3. Pilih folder Pengguna dan buka menu konteks (klik kanan). Pilih akun pengguna acak yang tercantum dalam panel kanan. Pilih Properti.
4. Pilih tab Akun. Di daftar Opsi akun, gulir ke bawah dan pastikan bahwa Tidak memerlukan preautentikasi Kerberos tidak dicentang.



Konfigurasikan forwarder bersyarat DNS untuk domain yang dikelola sendiri

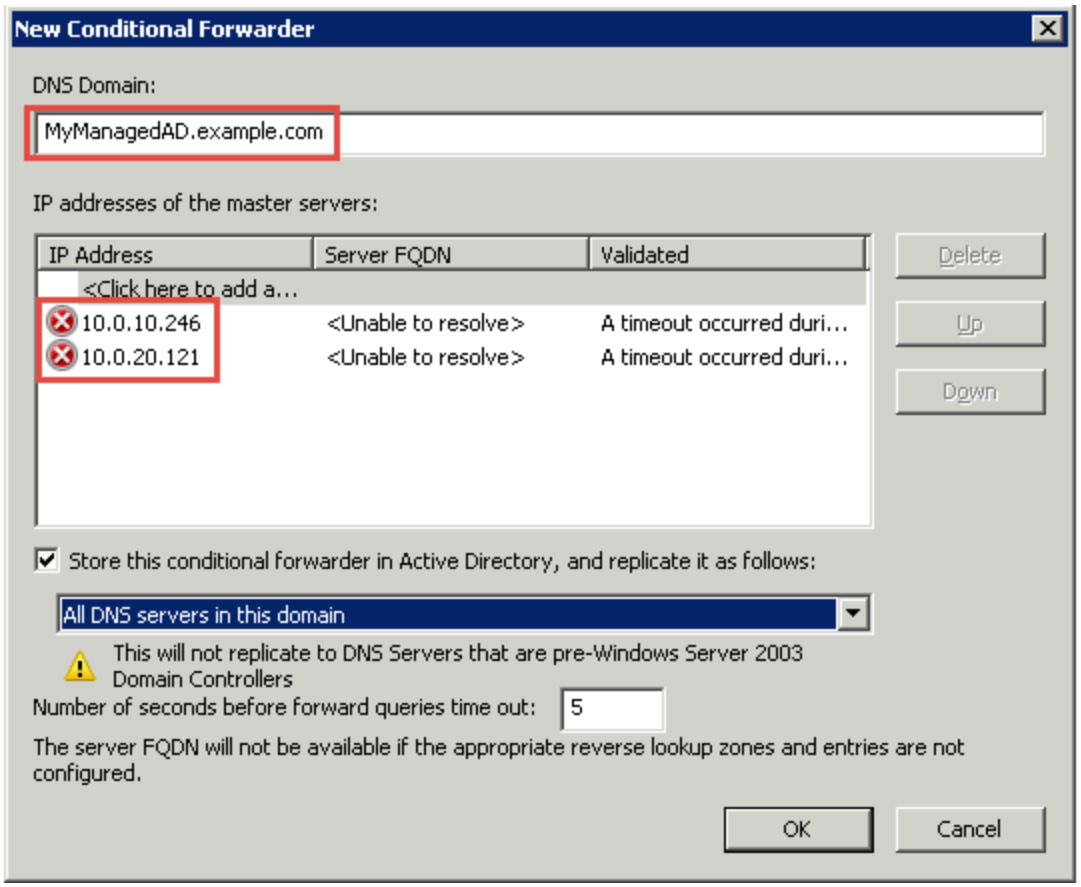
Anda harus mengatur penerusan bersyarat DNS pada setiap domain. Sebelum melakukan ini di domain yang dikelola sendiri, pertama-tama Anda akan mendapatkan beberapa informasi tentang iklan Microsoft yang AWS Dikelola.

Untuk mengonfigurasi forwarder bersyarat pada domain yang dikelola sendiri

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Di panel navigasi , pilih Direktori.
3. Pilih ID direktori iklan Microsoft AWS Terkelola Anda.
4. Pada halaman Detail, perhatikan nilai-nilai dalam Nama direktori dan Alamat DNS dari direktori Anda.
5. Sekarang, kembali ke pengontrol domain yang dikelola sendiri. Buka Pengelola Server
6. Pada menu Alat, pilih DNS.
7. Pada pohon konsol, perluas server DNS dari domain di mana Anda mengatur kepercayaan. Server kami adalah WIN-5V70CN7VJ0.corp.example.com.

8. Pada pohon konsol, pilih Penerusan Bersyarat.
9. Pada menu Tindakan, pilih Penerusan bersyarat baru.
10. Di domain DNS, ketik nama domain yang memenuhi syarat penuh (FQDN) dari AWS Microsoft AD Terkelola Anda, yang Anda sebutkan sebelumnya. Dalam contoh ini, FQDN adalah Ad.example.com. MyManaged
11. Pilih alamat IP server master dan ketik alamat DNS direktori Microsoft AD AWS Terkelola Anda, yang Anda catat sebelumnya. Dalam contoh ini yaitu: 10.0.10.246, 10.0.20.121

    Setelah memasukkan alamat DNS, Anda mungkin mendapatkan error “timeout” atau “tidak dapat menyelesaikan”. Anda biasanya dapat mengabaikan error ini.



12. Pilih Menyimpan penerusan bersyarat ini di Direktori Aktif dan mereplikasi sebagai berikut.
13. Pilih Semua server DNS dalam domain ini, lalu pilih OK.

Langkah Selanjutnya

[Langkah 2: Siapkan Microsoft AD yang Dikelola AWS]

Langkah 2: Siapkan Microsoft AD yang Dikelola AWS

Sekarang mari siapkan Microsoft AD yang Dikelola AWS untuk hubungan kepercayaan. Banyak dari langkah-langkah berikut hampir identik dengan apa yang baru saja Anda selesaikan untuk domain yang dikelola sendiri. Kali ini, bagaimanapun, Anda bekerja dengan Microsoft AD yang Dikelola AWS Anda.

Mengkonfigurasi subnet VPC dan grup keamanan Anda

Anda harus mengizinkan lalu lintas dari jaringan yang dikelola sendiri ke VPC yang berisi iklan Microsoft yang AWS Dikelola. Untuk melakukan ini, Anda perlu memastikan bahwa ACL yang diasosiasikan dengan subnet yang digunakan untuk men-deploy Microsoft AD yang Dikelola AWS dan aturan grup keamanan yang dikonfigurasi pada pengendali domain Anda, keduanya memungkinkan lalu lintas yang diperlukan untuk mendukung kepercayaan.

Persyaratan port bervariasi berdasarkan versi Windows Server yang digunakan oleh pengendali domain Anda dan layanan atau aplikasi yang akan memanfaatkan kepercayaan. Untuk tujuan tutorial ini, Anda harus membuka port-port berikut ini:

Ke dalam

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Autentikasi Kerberos
- TCP 636 - LDAPS (LDAP melalui TLS/SSL)
- TCP 3268-3269 - Katalog Global
- TCP/UDP 49152-65535 - Port-port sementara untuk RPC

> **Note**
>
> SMBv1 tidak lagi didukung.

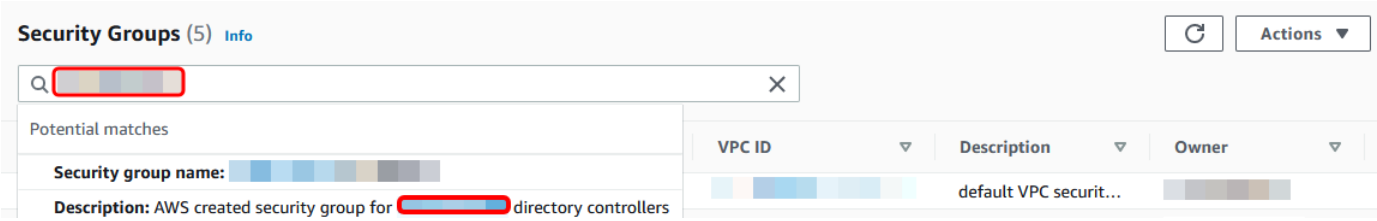
Ke luar

- SEMUA

> **Note**
>
> Ini adalah port minimum yang diperlukan untuk dapat menghubungkan VPC dan direktori yang dikelola sendiri. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Untuk mengkonfigurasi aturan keluar dan masuk pengendali domain Microsoft AD yang Dikelola AWS Anda.

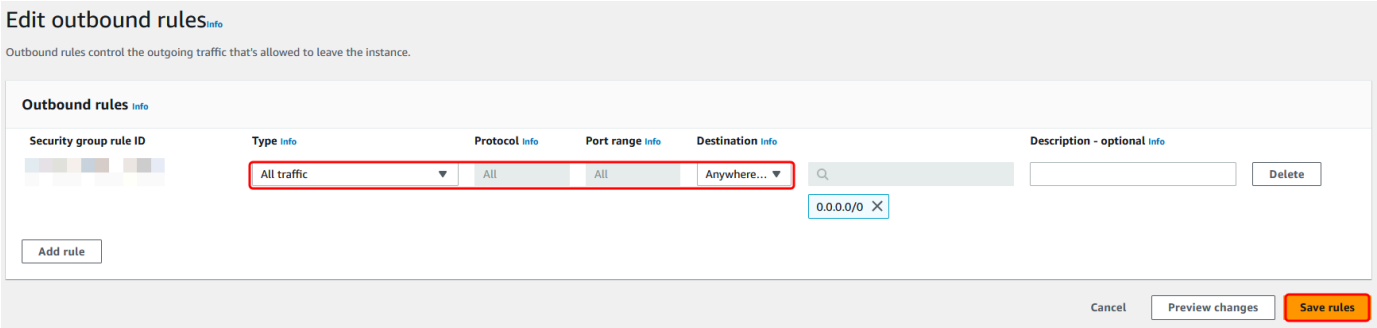
1. Kembali ke Konsol AWS Directory Service. Dalam daftar direktori, perhatikan ID direktori untuk direktori Microsoft AD yang Dikelola AWS.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih Grup Keamanan.
4. Gunakan kotak pencarian untuk mencari ID direktori Microsoft AD yang Dikelola AWS Anda. Dalam hasil pencarian, pilih Grup Keamanan dengan deskripsi**`AWS created security group for yourdirectoryID directory controllers`**.



5. Pergi ke tab Aturan Keluar untuk grup keamanan tersebut. Pilih Edit aturan keluar, lalu Tambahkan aturan. Untuk aturan baru, masukkan nilai berikut:

   - Jenis: SEMUA Lalu lintas
   - Protokol: SEMUA
   - Tujuan menentukan lalu lintas yang dapat meninggalkan pengendali domain Anda dan ke mana ia akan pergi. Tentukan alamat IP tunggal atau cakupan alamat IP dalam notasi CIDR (misalnya, 203.0.113.5/32). Anda juga dapat menentukan nama atau ID grup keamanan lain di Region yang sama. Untuk informasi selengkapnya, lihat Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan.

6. Pilih Simpan Aturan.

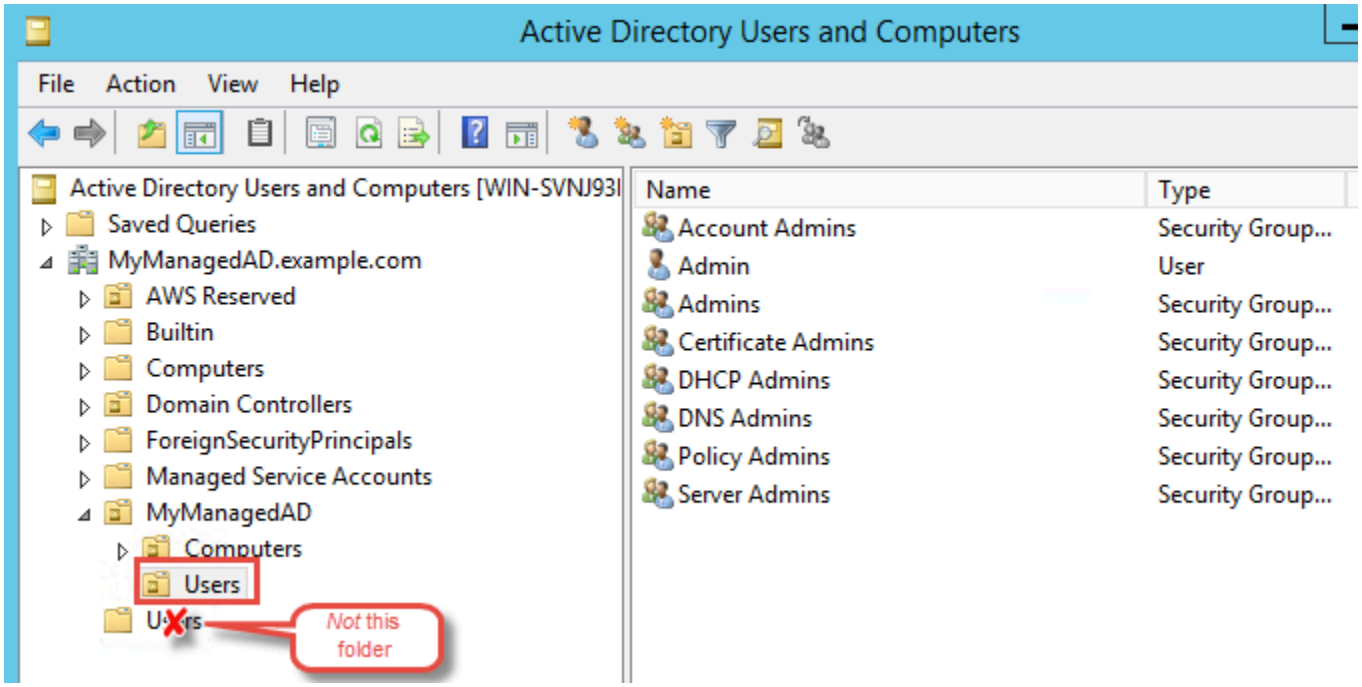


Pastikan bahwa Kerberos pra-autentikasi diaktifkan

Sekarang Anda ingin mengonfirmasi bahwa pengguna di Microsoft AD yang Dikelola AWS Anda juga telah mengaktifkan Kerberos pra-autentikasi. Ini adalah proses yang sama yang Anda selesaikan untuk direktori yang dikelola sendiri. Ini adalah default, tapi mari kita periksa untuk memastikan tidak ada yang berubah.

Untuk melihat pengaturan kerberos pengguna

1. Masuk ke instans yang merupakan anggota dari direktori Microsoft AD yang Dikelola AWS Anda menggunakan Izin untuk akun Administrator untuk domain atau akun yang telah didelegasikan izin untuk mengelola pengguna di domain.
2. Jika mereka belum diinstal, instal alat Pengguna dan Komputer Direktori Aktif dan alat DNS. Pelajari cara memasang alat ini di Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola.
3. Buka Pengelola Server Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
4. Pilih folder Pengguna di domain Anda. Perhatikan bahwa ini adalah folder Pengguna di bawah nama NetBIOS Anda, bukan folder Pengguna di bawah nama domain yang memenuhi syarat (FQDN).



5. Dalam daftar pengguna, klik kanan pada pengguna, dan kemudian pilih Properti.
6. Pilih tab Akun. Di daftar Opsi akun, pastikan bahwa Tidak memerlukan preautentikasi Kerberos tidak dicentang.

Langkah selanjutnya

Langkah 3: Buat hubungan kepercayaan

Langkah 3: Buat hubungan kepercayaan

Sekarang setelah persiapan selesai, langkah-langkah terakhir adalah membuat kepercayaan. Pertama, Anda membuat kepercayaan pada domain yang dikelola sendiri, dan akhirnya di Microsoft AD yang AWS Dikelola. Jika Anda memiliki masalah selama proses pembuatan kepercayaan, lihat Alasan status pembuatan kepercayaan untuk bantuan.

Konfigurasikan kepercayaan pada Direktori Aktif yang dikelola sendiri

Dalam tutorial ini, Anda mengkonfigurasi kepercayaan forest dua arah. Namun, jika Anda membuat kepercayaan forest satu arah, ketahui bahwa arah kepercayaan pada masing-masing domain Anda harus saling melengkapi. Misalnya, jika Anda membuat kepercayaan keluar satu arah pada domain yang dikelola sendiri, Anda perlu membuat kepercayaan masuk satu arah pada iklan AWS Microsoft yang Dikelola.

> **Note**
>
> Microsoft AD yang Dikelola AWS juga mendukung kepercayaan eksternal. Namun, untuk tujuan tutorial ini, Anda akan membuat kepercayaan forest dua arah.

Untuk mengonfigurasi kepercayaan pada Direktori Aktif yang dikelola sendiri

1. Buka Pengelola Server dan pada menu Alat, pilih Domain Direktori Aktif dan Kepercayaan.
2. Buka menu konteks (klik kanan) dari domain Anda dan pilih Properties.
3. Pilih tab Kepercayaan dan pilih Kepercayaan baru. Ketik nama dari Microsoft AD yang Dikelola AWS Anda dan pilih Selanjutnya.
4. Pilih Kepercayaan forest. Pilih Selanjutnya.
5. Pilih Dua arah. Pilih Selanjutnya.
6. Pilih Hanya domain ini. Pilih Selanjutnya.
7. Pilih Autentikasi seluruh forest. Pilih Selanjutnya.
8. Ketik Kata sandi kepercayaan. Pastikan untuk mengingat kata sandi ini karena Anda memerlukannya saat mengatur kepercayaan untuk Microsoft AD yang Dikelola AWS Anda.
9. Di kotak dialog berikutnya, konfirmasikan pengaturan Anda dan pilih Selanjutnya. Konfirmasikan bahwa kepercayaan telah dibuat dengan sukses dan pilih lagi Selanjutnya.
10. Pilih Tidak, jangan konfirmasikan kepercayaan keluar. Pilih Selanjutnya.
11. Pilih Tidak, jangan konfirmasikan kepercayaan masuk. Pilih Selanjutnya.

Konfigurasikan kepercayaan pada direktori Microsoft AD yang Dikelola AWS Anda.

Akhirnya, Anda mengkonfigurasi hubungan kepercayaan forest dengan direktori Microsoft AD yang Dikelola AWS. Karena Anda membuat trust hutan dua arah pada domain yang dikelola sendiri, Anda juga membuat kepercayaan dua arah menggunakan direktori AWS Microsoft AD yang Dikelola.

> **Note**
>
> Hubungan kepercayaan adalah fitur global dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus dilakukan di Region primer. Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk mengkonfigurasi kepercayaan pada direktori Microsoft AD yang Dikelola AWS Anda.

1. Kembali ke Konsol AWS Directory Service.
2. Pilih halaman Direktori, pilih ID Microsoft AD yang Dikelola AWS Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Pada halaman Tambahkan hubungan kepercayaan, tentukan jenis Trust. Dalam hal ini, kami memilih kepercayaan Hutan. Ketik FQDN domain yang dikelola sendiri (dalam tutorial ini). **`corp.example.com`** Ketik kata sandi kepercayaan yang sama dengan yang Anda gunakan saat membuat kepercayaan pada domain yang dikelola sendiri. Tentukan arah. Dalam hal ini, kami memilih Dua arah.
6. Di bidang Conditional forwarder, masukkan alamat IP server DNS yang dikelola sendiri. Dalam contoh ini, masukkan 172.16.10.153.
7. (Opsional) Pilih Tambahkan alamat IP lain dan masukkan alamat IP kedua untuk server DNS yang dikelola sendiri. Anda dapat menentukan hingga total empat server DNS.
8. Pilih Tambahkan.

Selamat. Anda sekarang memiliki hubungan kepercayaan antara domain yang dikelola sendiri (corp.example.com) dan iklan AWS Microsoft Terkelola (Ad.example.com). MyManaged Hanya satu hubungan yang dapat diatur antara kedua domain ini. Jika misalnya, Anda ingin mengubah arah kepercayaan ke satu arah, Anda harus terlebih dahulu menghapus hubungan kepercayaan yang ada ini dan membuat yang baru.

Untuk informasi selengkapnya, termasuk petunjuk tentang memverifikasi atau menghapus kepercayaan, lihat Menciptakan hubungan kepercayaan.

Tutorial: Membuat hubungan kepercayaan antara duaAWSDomain Microsoft AD yang Dikelola

Tutorial ini memandu Anda melalui semua langkah yang diperlukan untuk mengatur hubungan kepercayaan antara duaAWSDirectory Service untuk Microsoft Active Directory domain.

Topik

- Langkah 1: Siapkan Microsoft AD yang AWS Dikelola
- Langkah 2: Membuat hubungan kepercayaan dengan yang lainAWSDomain Microsoft AD yang Dikelola

Lihat Juga

Menciptakan hubungan kepercayaan

Langkah 1: Siapkan Microsoft AD yang AWS Dikelola

Di bagian ini, Anda akan menyiapkan iklan Microsoft AWS Terkelola untuk hubungan kepercayaan dengan iklan Microsoft AWS Terkelola lainnya. Banyak dari langkah-langkah berikut hampir identik dengan apa yang Anda lakukanTutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri. Namun, kali ini, Anda mengonfigurasi lingkungan Microsoft AD yang AWS Dikelola agar berfungsi satu sama lain.

Mengkonfigurasi subnet VPC dan grup keamanan Anda

Anda harus mengizinkan lalu lintas dari satu jaringan Microsoft AD AWS Terkelola ke VPC yang berisi iklan AWS Microsoft Terkelola lainnya. Untuk melakukan ini, Anda perlu memastikan bahwa ACL yang diasosiasikan dengan subnet yang digunakan untuk men-deploy Microsoft AD yang Dikelola AWS dan aturan grup keamanan yang dikonfigurasi pada pengendali domain Anda, keduanya memungkinkan lalu lintas yang diperlukan untuk mendukung kepercayaan.

Persyaratan port bervariasi berdasarkan versi Windows Server yang digunakan oleh pengendali domain Anda dan layanan atau aplikasi yang akan memanfaatkan kepercayaan. Untuk tujuan tutorial ini, Anda harus membuka port-port berikut ini:

Ke dalam

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos

- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

> **Note**
>
> SMBv1 tidak lagi didukung.

- TCP/UDP 464 - Autentikasi Kerberos
- TCP 636 - LDAPS (LDAP melalui TLS/SSL)
- TCP 3268-3269 - Katalog Global
- TCP/UDP 1024-65535 - Port sementara untuk RPC

Ke luar

- SEMUA

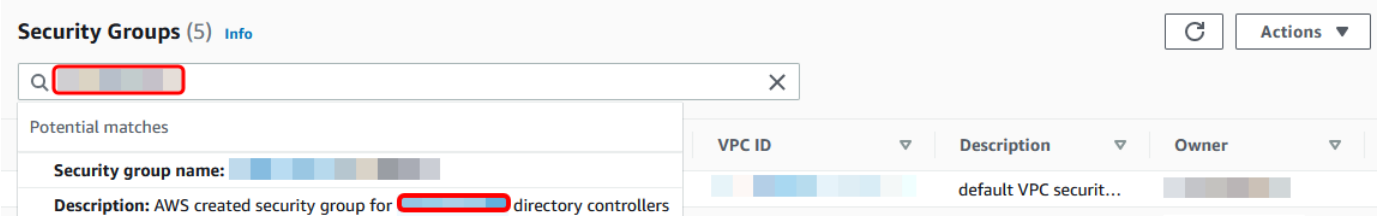
> **Note**
>
> Ini adalah port minimum yang diperlukan untuk dapat menghubungkan VPC dari kedua Microsoft AD yang AWS Dikelola. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka. Untuk informasi selengkapnya, lihat Cara mengonfigurasi firewall untuk domain dan trust Active Directory di situs web Microsoft.

Untuk mengonfigurasi aturan keluar pengontrol domain Microsoft AD AWS Terkelola

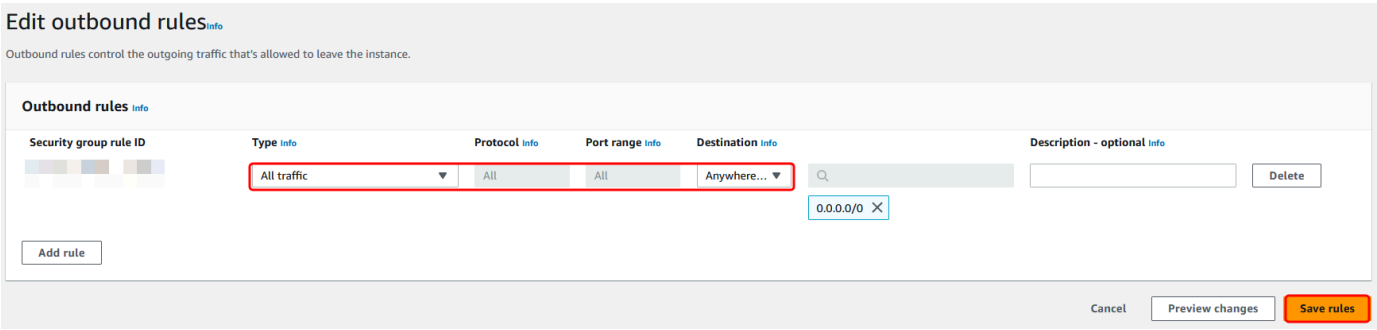
> **Note**
>
> Ulangi langkah 1-6 di bawah ini untuk setiap direktori.

1. Pergi ke AWS Directory Servicekonsol. Dalam daftar direktori, perhatikan ID direktori untuk direktori Microsoft AD yang Dikelola AWS.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

3. Di panel navigasi, pilih Grup Keamanan.
4. Gunakan kotak pencarian untuk mencari ID direktori Microsoft AD yang Dikelola AWS Anda. Dalam hasil pencarian, pilih item dengan deskripsi**`AWS created security group for yourdirectoryID directory controllers`**.



5. Pergi ke tab Aturan Keluar untuk grup keamanan tersebut. Pilih Edit, kemudian Tambahkan aturan lain. Untuk aturan baru, masukkan nilai berikut:
   - Jenis: SEMUA Lalu lintas
   - Protokol: SEMUA
   - Tujuan menentukan lalu lintas yang dapat meninggalkan pengendali domain Anda dan ke mana ia akan pergi. Tentukan alamat IP tunggal atau cakupan alamat IP dalam notasi CIDR (misalnya, 203.0.113.5/32). Anda juga dapat menentukan nama atau ID grup keamanan lain di Region yang sama. Untuk informasi selengkapnya, lihat Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan.
6. Pilih Simpan.

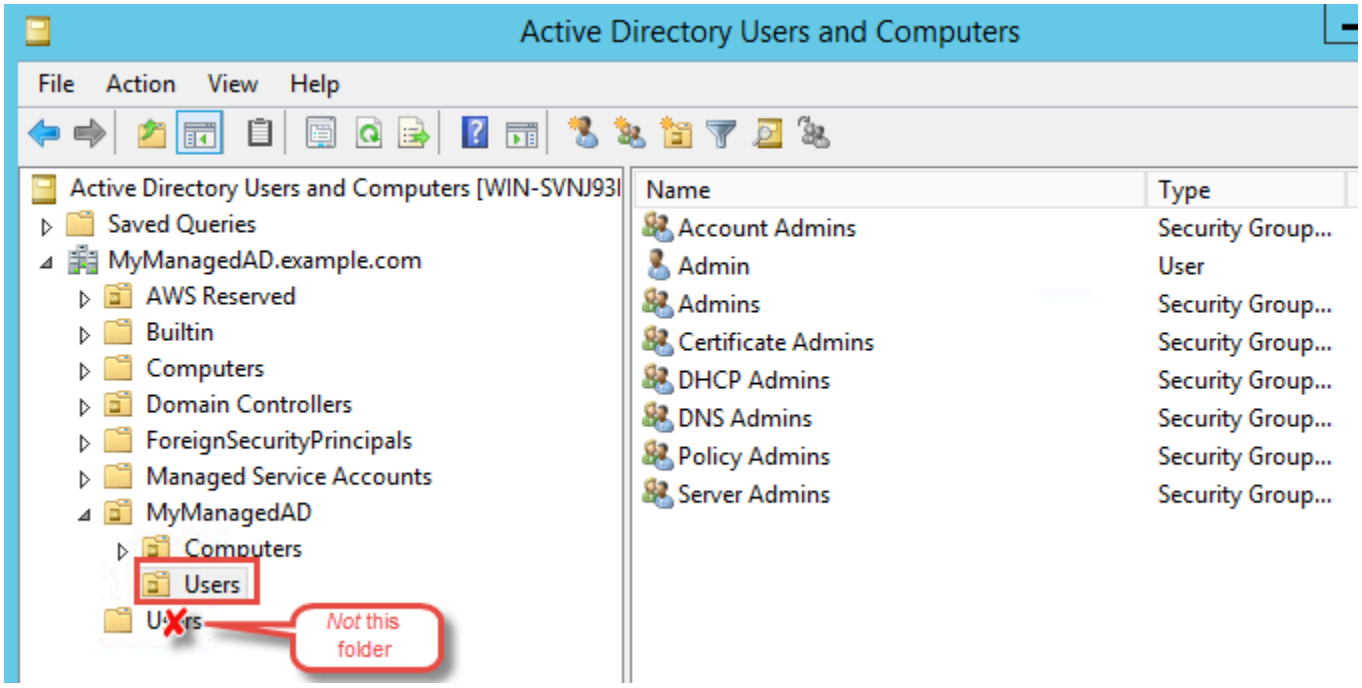


Pastikan bahwa Kerberos pra-autentikasi diaktifkan

Sekarang Anda ingin mengonfirmasi bahwa pengguna di Microsoft AD yang Dikelola AWS Anda juga telah mengaktifkan Kerberos pra-autentikasi. Ini adalah proses yang sama yang Anda selesaikan untuk direktori on-premise Anda. Ini adalah default, tapi mari kita periksa untuk memastikan tidak ada yang berubah.

Untuk melihat pengaturan kerberos pengguna

1. Masuk ke instans yang merupakan anggota dari direktori Microsoft AD yang Dikelola AWS Anda menggunakan Izin untuk akun Administrator untuk domain atau akun yang telah didelegasikan izin untuk mengelola pengguna di domain.
2. Jika mereka belum diinstal, instal alat Pengguna dan Komputer Direktori Aktif dan alat DNS. Pelajari cara memasang alat ini di Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola.
3. Buka Pengelola Server Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
4. Pilih folder Pengguna di domain Anda. Perhatikan bahwa ini adalah folder Pengguna di bawah nama NetBIOS Anda, bukan folder Pengguna di bawah nama domain yang memenuhi syarat (FQDN).



5. Dalam daftar pengguna, klik kanan pada pengguna, dan kemudian pilih Properti.
6. Pilih tab Akun. Di daftar Opsi akun, pastikan bahwa Tidak memerlukan preautentikasi Kerberos tidak dicentang.

Langkah selanjutnya

Langkah 2: Membuat hubungan kepercayaan dengan yang lainAWSDomain Microsoft AD yang Dikelola

Langkah 2: Membuat hubungan kepercayaan dengan yang lainAWSDomain Microsoft AD yang Dikelola

Sekarang setelah persiapan selesai, langkah terakhir adalah membuat kepercayaan di antara keduanyaAWSDomain Microsoft AD yang Dikelola. Jika Anda memiliki masalah selama proses pembuatan kepercayaan, lihat Alasan status pembuatan kepercayaan untuk bantuan.

Konfigurasikan kepercayaan di pertama AndaAWSDomain Microsoft AD yang Dikelola

Dalam tutorial ini, Anda mengkonfigurasi kepercayaan forest dua arah. Namun, jika Anda membuat kepercayaan forest satu arah, ketahui bahwa arah kepercayaan pada masing-masing domain Anda harus saling melengkapi. Misalnya, jika Anda membuat kepercayaan keluar, satu arah di domain pertama ini, Anda harus membuat kepercayaan masuk, satu arah di kedua Anda.AWSDomain Microsoft AD yang Dikelola.

> **Note**
>
> Microsoft AD yang Dikelola AWS juga mendukung kepercayaan eksternal. Namun, untuk tujuan tutorial ini, Anda akan membuat kepercayaan forest dua arah.

Untuk mengkonfigurasi kepercayaan di pertama AndaAWSDomain Microsoft AD yang Dikelola

1. Buka konsol AWS Directory Service.
2. PadaDirektorihalaman, pilih yang pertamaAWSMicrosoft AD yang Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. PadaTambahkan hubungan kepercayaanhalaman, Ketik FQDN keduaAWSDomain Microsoft AD yang Dikelola. Pastikan untuk mengingat kata sandi ini karena Anda memerlukannya saat mengatur kepercayaan untuk kedua AndaAWSMicrosoft AD yang Dikelola. Tentukan arah. Dalam hal ini, pilihDua arah.

6. DiForwarder bersyaratbidang, masukkan alamat IP kedua AndaAWSServer Microsoft AD yang Dikelola.
7. (Opsional) PilihTambahkan alamat IP lainnyadan masukkan alamat IP kedua untuk keduaAWSServer Microsoft AD yang Dikelola. Anda dapat menentukan hingga total empat server DNS.
8. Pilih Tambahkan. Kepercayaan akan gagal pada titik ini yang diharapkan sampai kita menciptakan sisi lain dari kepercayaan.

Konfigurasikan kepercayaan di kedua AndaAWSDomain Microsoft AD yang Dikelola

Sekarang, Anda mengkonfigurasi hubungan kepercayaan hutan dengan hubungan kedua AndaAWSDirektori Microsoft AD yang Dikelola. Karena Anda membuat kepercayaan dua arah di hutan pertamaAWSDomain Microsoft AD yang dikelola, Anda juga membuat kepercayaan dua arah menggunakan iniAWSDomain Microsoft AD yang Dikelola.

Untuk mengkonfigurasi kepercayaan di kedua AndaAWSDomain Microsoft AD yang Dikelola

1. Kembali ke Konsol AWS Directory Service.
2. PadaDirektorihalaman, pilih keduaAWSMicrosoft AD yang Dikelola.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. PadaTambahkan hubungan kepercayaanhalaman, Ketik FQDN pertama AndaAWSDomain Microsoft AD yang Dikelola. Ketik kata sandi kepercayaan yang sama yang Anda gunakan saat membuat kepercayaan pada domain on-premise Anda. Tentukan arah. Dalam hal ini, pilihDua arah.
6. DiForwarder bersyaratbidang, masukkan alamat IP pertama AndaAWSServer Microsoft AD yang Dikelola.

7. (Opsional) PilihTambahkan alamat IP lainnyadan masukkan alamat IP kedua untuk pertamaAWSServer Microsoft AD yang Dikelola. Anda dapat menentukan hingga total empat server DNS.
8. Pilih Tambahkan. Kepercayaan harus diverifikasi segera setelah itu.
9. Sekarang, kembali ke kepercayaan yang Anda buat di domain pertama dan verifikasi hubungan kepercayaan lagi.

Selamat. Anda sekarang memiliki hubungan kepercayaan antara keduanyaAWSDomain Microsoft AD yang Dikelola. Hanya satu hubungan yang dapat diatur antara kedua domain ini. Jika misalnya, Anda ingin mengubah arah kepercayaan ke satu arah, Anda harus terlebih dahulu menghapus hubungan kepercayaan yang ada ini dan membuat yang baru.

Perpanjang skema Anda

Microsoft AD yang Dikelola AWS menggunakan skema untuk mengatur dan menerapkan bagaimana data direktori disimpan. Proses menambahkan definisi skema disebut sebagai “memperluas skema.” Ekstensi skema memungkinkan Anda untuk memodifikasi skema dari Microsoft AD yang Dikelola AWS Anda menggunakan file LDAP Data Interchange Format (LDIF) yang valid. Untuk informasi lebih lanjut tentang skema AD dan cara untuk memperluas skema Anda, lihat topik yang tercantum di bawah ini.

Topik

- Kapan harus memperpanjang skema Microsoft AD yang Dikelola AWS Anda
- Tutorial: Memperluas skema AD Microsoft yang AWS Dikelola

Kapan harus memperpanjang skema Microsoft AD yang Dikelola AWS Anda

Anda dapat memperpanjang skema Microsoft AD yang Dikelola AWS Anda dengan menambahkan kelas objek baru dan atribut. Misalnya, Anda mungkin melakukan ini jika Anda memiliki aplikasi yang memerlukan perubahan pada skema Anda untuk mendukung kemampuan sign-on tunggal.

Anda juga dapat menggunakan ekstensi skema untuk mengaktifkan dukungan untuk aplikasi yang bergantung pada kelas objek Direktori Aktif tertentu dan atribut. Hal ini dapat sangat berguna dalam kasus di mana Anda perlu memigrasikan aplikasi perusahaan yang bergantung pada Microsoft AD yang Dikelola AWS, ke cloud AWS.

Setiap atribut atau kelas yang ditambahkan ke skema Direktori Aktif yang ada harus didefinisikan dengan ID unik. Dengan begitu ketika perusahaan menambahkan ekstensi ke skema, mereka dapat dijamin unik dan tidak bertentangan satu sama lain. ID ini disebut sebagai Pengidentifikasi Objek AD (OIDs) dan disimpan di Microsoft AD yang Dikelola AWS.

Untuk memulai, lihat Tutorial: Memperluas skema AD Microsoft yang AWS Dikelola.

Topik terkait

- Perpanjang skema Anda
- Elemen skema

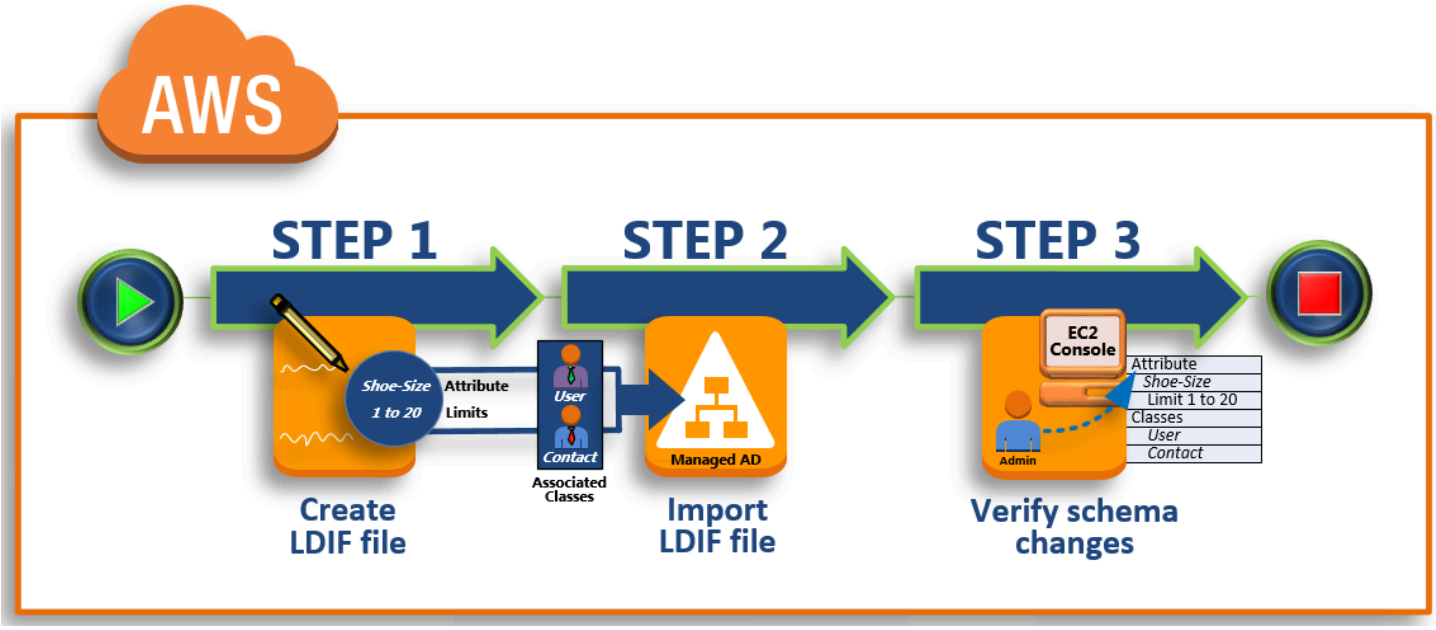
Tutorial: Memperluas skema AD Microsoft yang AWS Dikelola

Dalam tutorial ini, Anda akan belajar cara memperluas skema untuk AWS direktori Directory Service for Microsoft Active Directory Anda, juga dikenal sebagai AWS Managed Microsoft AD, dengan menambahkan atribut dan kelas unik yang memenuhi persyaratan spesifik Anda. AWS Ekstensi skema Microsoft AD yang dikelola hanya dapat diunggah dan diterapkan menggunakan file skrip LDIF (Lightweight Directory Interchange Format) yang valid.

Atribut (attributeSchema) menentukan bidang dalam database sementara kelas (classSchema) menentukan tabel dalam database. Sebagai contoh, semua objek pengguna di Direktori Aktif ditentukan oleh kelas skema Pengguna sedangkan properti individu pengguna, seperti alamat email atau nomor telepon, masing-masing ditentukan oleh atribut.

Jika Anda ingin menambahkan properti baru, seperti Shoe-Size, Anda akan menentukan atribut baru, yang akan menjadi tipe integer. Anda juga bisa menentukan batas bawah dan atas seperti 1 sampai 20. Setelah objek Shoe-size attributeSchema telah dibuat, Anda kemudian akan mengubah objek classSchema Pengguna untuk memuat atribut itu. Atribut dapat ditautkan ke beberapa kelas. Shoe-size juga dapat ditambahkan ke kelas Kontak misalnya. Untuk informasi selengkapnya tentang skema Direktori Aktif, lihat Kapan harus memperpanjang skema Microsoft AD yang Dikelola AWS Anda.

Alur kerja ini memiliki tiga langkah dasar.



Langkah 1: Buat file LDIF Anda

Pertama, Anda membuat file LDIF dan tentukan atribut baru dan setiap kelas yang atribut harus ditambahkan ke. Anda menggunakan file ini untuk tahap berikutnya dari alur kerja.

Langkah 2: Impor file LDIF Anda

Pada langkah ini, Anda menggunakan AWS Directory Service konsol untuk mengimpor file LDIF ke lingkungan Microsoft Active Directory Anda.

Langkah 3: Verifikasi apakah ekstensi skema berhasil

Akhirnya, sebagai administrator, Anda menggunakan instans EC2 untuk memverifikasi bahwa ekstensi baru muncul di Snap-in skema Direktori Aktif.

Langkah 1: Buat file LDIF Anda

Sebuah file LDIF adalah format pertukaran data teks biasa standar untuk mewakili konten direktori LDAP (Lightweight Directory Access Protocol) dan permintaan pembaruan. LDIF menyampaikan konten direktori sebagai satu set catatan, satu catatan untuk setiap objek (atau entri). Hal ini juga merupakan permintaan pembaruan, seperti Menambahkan, Memodifikasi, Menghapus, dan Mengubah nama, sebagai satu set catatan, satu catatan untuk setiap permintaan pembaruan.

AWS Directory Service Mengimpor file LDIF Anda dengan skema berubah dengan menjalankan `ldifde.exe` aplikasi di direktori AWS Microsoft AD Terkelola Anda. Oleh karena itu, Anda akan

merasa terbantu untuk memahami sintaks skrip LDIF. Untuk informasi selengkapnya, lihat.Skrip LDIF.

Beberapa alat LDIF pihak ketiga dapat mengekstrak, membersihkan, dan memperbarui pembaruan skema Anda. Terlepas dari alat yang Anda gunakan, penting untuk memahami bahwa semua pengidentifikasi yang digunakan dalam file LDIF Anda harus unik.

Kami sangat menyarankan Anda meninjau konsep-konsep berikut dan tips sebelum membuat file LDIF Anda.

- Elemen skema – Pelajari tentang elemen skema seperti atribut, kelas, ID objek, dan atribut tertaut. Untuk informasi selengkapnya, lihat Elemen skema.

- Urutan item – Pastikan bahwa urutan di mana item dalam file LDIF Anda ditata mengikuti Pohon Informasi Direktori (DIT) dari atas ke bawah. Aturan umum untuk pengurutan dalam file LDIF meliputi hal berikut ini:

  - Pisahkan item dengan garis kosong.
  - Buat daftar item anak setelah item induknya.
  - Pastikan bahwa item seperti atribut atau kelas objek ada di dalam skema. Jika mereka tidak ada, Anda harus menambahkannya ke skema sebelum mereka dapat digunakan. Misalnya, sebelum Anda dapat menetapkan atribut ke kelas, atribut harus dibuat.

- Format DN – Untuk setiap instruksi baru dalam file LDIF, tentukan nama yang dibedakan (DN) sebagai baris pertama dari instruksi. DN mengidentifikasi objek Direktori Aktif dalam pohon objek Direktori Aktif dan harus berisi komponen domain untuk direktori Anda. Sebagai contoh, komponen domain untuk direktori dalam tutorial ini adalah `DC=example,DC=com`.

  DN juga harus berisi nama umum (CN) dari objek Direktori Aktif. Entri CN pertama adalah atribut atau nama kelas. Selanjutnya, Anda harus menggunakan `CN=Schema,CN=Configuration`. CN ini memastikan bahwa Anda dapat memperluas skema Direktori Aktif. Seperti yang disebutkan sebelumnya, Anda tidak dapat menambah atau memodifikasi konten objek Direktori Aktif. Format umum untuk DN berikut.

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  Untuk tutorial ini, DN untuk atribut Shoe-Size baru akan terlihat seperti:

```
dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
```

- Peringatan – Tinjau peringatan di bawah ini sebelum Anda memperpanjang skema Anda.
  - Sebelum Anda memperpanjang skema Direktori Aktif Anda, penting untuk meninjau peringatan Microsoft pada dampak operasi ini. Untuk informasi selengkapnya, lihat Apa yang Harus Anda Ketahui Sebelum Memperluas Skema.
  - Anda tidak dapat menghapus atribut skema atau kelas. Oleh karena itu, jika Anda membuat kesalahan dan tidak ingin memulihkan dari backup, Anda hanya dapat menonaktifkan objek tersebut. Untuk informasi selengkapnya, lihat Menonaktifkan Kelas dan Atribut yang Ada.
  - Perubahan defaultSecurityDescriptor tidak didukung.

Untuk mempelajari selengkapnya tentang cara file LDIF dibuat dan melihat contoh file LDIF yang dapat digunakan untuk menguji ekstensi skema AWS Microsoft AD Terkelola, lihat artikel Cara Memperluas Skema Direktori AWS Microsoft AD Terkelola Anda di Blog Keamanan. AWS

Langkah Selanjutnya

Langkah 2: Impor file LDIF Anda

Langkah 2: Impor file LDIF Anda

Anda dapat memperluas skema Anda dengan mengimpor file LDIF baik dari AWS Directory Service konsol atau dengan menggunakan API. Untuk informasi selengkapnya tentang cara melakukannya dengan ekstensi skema API, lihat Referensi API AWS Directory Service . Pada saat ini, AWS tidak mendukung aplikasi eksternal, seperti Microsoft Exchange, untuk melakukan pembaruan skema secara langsung.

> **Important**
>
> Saat Anda membuat pembaruan ke skema direktori Microsoft AD AWS Terkelola, operasi tidak dapat dibalik. Dengan kata lain, setelah Anda membuat kelas baru atau atribut, Direktori Aktif tidak mengizinkan Anda untuk menghapusnya. Namun, Anda dapat menonaktifkannya. Jika Anda harus menghapus perubahan skema, salah satu pilihan adalah untuk memulihkan direktori dari snapshot sebelumnya. Memulihkan snapshot mengembalikan skema dan data direktori kembali ke titik sebelumnya, bukan hanya skema. Perhatikan, usia maksimum yang didukung dari snapshot adalah 180 hari. Untuk informasi selengkapnya, lihat Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif di situs web Microsoft.

Sebelum proses pembaruan dimulai, Microsoft AD yang AWS dikelola mengambil snapshot untuk mempertahankan status direktori Anda saat ini.

> **Note**
>
> Ekstensi skema adalah fitur global dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus dilakukan di Region primer. Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk mengimpor file LDIF Anda

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Pemeliharaan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pemeliharaan.
4. Di bagian Ekstensi skema, pilih Tindakan, dan kemudian pilih Unggah dan perbarui skema.
5. Di kotak dialog, klik Browse, pilih file LDIF yang valid, ketik deskripsi, dan kemudian pilih Memperbarui skema.

> **Important**
>
> Memperpanjang skema adalah operasi kritis. Jangan menerapkan pembaruan skema dalam lingkungan produksi tanpa terlebih dahulu menguji dengan aplikasi Anda dalam pengembangan atau pengujian lingkungan.

Bagaimana file LDIF diterapkan

Setelah file LDIF Anda diunggah, AWS Microsoft AD yang Dikelola mengambil langkah-langkah untuk melindungi direktori Anda dari kesalahan karena menerapkan perubahan dalam urutan berikut.

1. Memvalidasi file LDIF. Karena skrip LDIF dapat memanipulasi objek apa pun di domain, AWS Microsoft AD yang Dikelola menjalankan pemeriksaan tepat setelah Anda mengunggah untuk membantu memastikan bahwa operasi impor tidak akan gagal. Hal ini termasuk pemeriksaan untuk memastikan hal berikut:
   - Objek yang akan diperbarui hanya diadakan dalam kotainer skema
   - Bagian DC (pengendali domain) cocok dengan nama domain di mana skrip LDIF berjalan
2. Mengambil snapshot dari direktori Anda. Anda dapat menggunakan snapshot tersebut untuk memulihkan direktori Anda jika Anda mengalami masalah dengan aplikasi Anda setelah memperbarui skema.
3. Menerapkan perubahan ke DC tunggal. AWS Microsoft AD yang dikelola mengisolasi salah satu DC Anda dan menerapkan pembaruan dalam file LDIF ke DC yang terisolasi. Kemudian memilih salah satu DC Anda menjadi skema utama, menghapus DC tersebut dari replikasi direktori, dan menerapkan file LDIF Anda menggunakan `Ldifde.exe`.
4. Replikasi terjadi pada semua DC. AWS Microsoft AD yang dikelola menambahkan DC yang terisolasi kembali ke replikasi untuk menyelesaikan pembaruan. Saat ini semua terjadi, direktori Anda terus menyediakan layanan Direktori Aktif untuk aplikasi Anda tanpa gangguan.

Langkah selanjutnya

Langkah 3: Verifikasi apakah ekstensi skema berhasil

Langkah 3: Verifikasi apakah ekstensi skema berhasil

Setelah Anda menyelesaikan proses impor, penting untuk memverifikasi bahwa pembaruan skema diterapkan ke direktori Anda. Hal ini sangat penting sebelum Anda bermigrasi atau memperbarui aplikasi yang bergantung pada pembaruan skema. Anda dapat melakukannya dengan menggunakan berbagai alat LDAP yang berbeda atau dengan menulis alat uji yang mengeluarkan perintah LDAP yang sesuai.

Prosedur ini menggunakan Active Directory Schema Snap-in dan/atau PowerShell untuk memverifikasi bahwa pembaruan skema diterapkan. Anda harus menjalankan alat ini dari komputer yang merupakan domain yang bergabung dengan iklan Microsoft AWS Terkelola Anda. Ini bisa berupa server Windows yang berjalan di jaringan on-premise Anda dengan akses ke virtual private cloud (VPC) Anda atau melalui koneksi virtual private network (VPN). Anda juga dapat menjalankan alat ini pada instans Windows Amazon EC2 (lihat Cara untuk meluncurkan instans EC2 baru dengan bergabung domain mulus).

Untuk memverifikasi menggunakan Snap-in skema Direktori Aktif

1. Instal Skema Direktori Aktif Snap-In menggunakan instruksi di situs web. TechNet
2. Buka Konsol Manajemen Microsoft (MMC) dan perluas pohon Skema AD untuk direktori Anda.
3. Navigasikan melalui folder Kelas dan Atribut sampai Anda menemukan perubahan skema yang Anda buat sebelumnya.

Untuk memverifikasi menggunakan PowerShell

1. Buka PowerShell jendela.
2. Gunakan `Get-ADObject` seperti yang ditunjukkan di bawah ini untuk memverifikasi perubahan skema. Sebagai contoh:

```
get-adobject -Identity 'CN=Shoe-
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

Langkah opsional

Tambahkan nilai ke atribut baru - Opsional

Tambahkan nilai ke atribut baru - Opsional

Gunakan langkah opsional ini ketika Anda telah membuat atribut baru dan ingin menambahkan nilai baru ke atribut di direktori Microsoft AD yang AWS Dikelola.

Untuk menambahkan nilai ke atribut

1. Buka utilitas baris Windows PowerShell perintah dan atur atribut baru dengan perintah berikut. Dalam contoh ini, kita akan menambahkan nilai EC2InstanceID baru ke atribut untuk komputer tertentu.

```
PS C:\> set-adcomputer -Identity computer name -add @{example-
EC2InstanceID = 'EC2 instance ID'}
```

2. Anda dapat memvalidasi jika nilai EC2InstanceID ditambahkan ke objek komputer dengan menjalankan perintah berikut:

```
PS C:\> get-adcomputer -Identity computer name –Property example-
EC2InstanceID
```

Sumber daya terkait

Tautan sumber daya berikut terletak di situs web Microsoft dan memberikan informasi terkait.

- Memperluas Skema (Windows)
- Skema Direktori Aktif (Windows)
- Skema Direktori Aktif
- Administrasi Windows: Memperluas Skema Direktori Aktif
- Pembatasan pada Ekstensi Skema (Windows)
- Ldifde

Pertahankan direktori Microsoft AD yang AWS Dikelola

Bagian ini menjelaskan cara mempertahankan tugas administratif umum untuk lingkungan Microsoft AD AWS Terkelola Anda.

Topik

- Menambahkan akhiran UPN alternatif
- Menghapus iklan Microsoft yang AWS Dikelola
- Ganti nama situs direktori Anda
- Snapshot atau pulihkan direktori Anda
- Tingkatkan Direktori Aktif Microsoft AD AWS Terkelola
- Melihat informasi direktori

Menambahkan akhiran UPN alternatif

Anda dapat menyederhanakan pengelolaan nama login Direktori Aktif (AD) dan meningkatkan pengalaman login pengguna dengan menambahkan akhiran nama dasar pengguna (UPN) alternatif ke direktori Microsoft AD yang Dikelola AWS Anda. Untuk melakukan itu, Anda harus masuk dengan akun Admin atau dengan akun yang merupakan anggota dari grup Administrator Akhiran Nama Dasar Pengguna yang Didelegasikan AWS. Untuk informasi selengkapnya tentang grup ini, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.

Untuk menambahkan akhiran UPN alternatif

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Temukan instans Amazon EC2 yang digabungkan ke direktori Microsoft AD yang Dikelola AWS Anda. Pilih instans, lalu pilih Hubungkan.
3. Di jendela Pengelola Server, pilih Alat. Lalu pilih Domain Direktori Aktif dan Kepercayaan.
4. Di panel sebelah kiri, klik kanan Domain Direktori Aktif dan Kepercayaan lalu pilih Properti.
5. Di tab Akhiran UPN, ketik alternatif akhiran UPN (seperti **`sales.example.com`**). Pilih Tambahkan , lalu pilih Terapkan .
6. Jika Anda perlu menambahkan akhiran UPN alternatif tambahan, ulangi langkah 5 sampai Anda memiliki akhiran UPN yang Anda butuhkan.

Menghapus iklan Microsoft yang AWS Dikelola

Ketika iklan Microsoft AWS Terkelola dihapus, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instans yang bergabung ke direktori tetap utuh. Anda tidak dapat, bagaimanapun, menggunakan kredensial direktori Anda untuk masuk ke instans ini. Anda harus log in ke instans ini dengan akun pengguna yang lokal untuk instans.

Untuk menghapus direktori

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori. Pastikan Anda berada di Wilayah AWS tempat Anda Active Directory dikerahkan. Untuk informasi selengkapnya, lihat Memilih Wilayah.
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk direktori yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus iklan Microsoft AWS Terkelola atau Simple AD Anda.

   a. Pada halaman Direktori, pilih ID direktori Anda.

   b. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk direktori Anda.

      - Nonaktifkan AWS Management Console akses.
      - Untuk menonaktifkan Amazon WorkSpaces, Anda harus membatalkan pendaftaran layanan dari direktori di konsol. WorkSpaces Untuk informasi selengkapnya, lihat membatalkan pendaftaran dari direktori di Panduan Administrasi Amazon WorkSpaces .

- Untuk menonaktifkan Amazon WorkDocs, Anda harus menghapus WorkDocs situs Amazon di WorkDocs konsol Amazon. Untuk informasi selengkapnya, lihat Menghapus situs di Panduan WorkDocs Administrasi Amazon.
- Untuk menonaktifkan Amazon WorkMail, Anda harus menghapus WorkMail organisasi Amazon di WorkMail konsol Amazon. Untuk informasi selengkapnya, lihat Menghapus organisasi di Panduan WorkMail Administrator Amazon.
- Untuk menonaktifkan Amazon FSx for Windows File Server, Anda harus menghapus sistem file Amazon FSx dari domain. Untuk informasi selengkapnya, lihat Bekerja dengan Active Directory di FSx for Windows File Server di Panduan Pengguna Amazon FSx for Windows File Server.
- Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat Mengelola instans DB dalam domain dalam Panduan Pengguna Amazon RDS.
- Untuk menonaktifkan AWS Client VPN Layanan, Anda harus menghapus layanan direktori dari Endpoint Client VPN. Untuk informasi selengkapnya, lihat Active DirectoryOtentikasi di Panduan AWS Client VPN Administrator.
- Untuk menonaktifkan Amazon Connect, Anda harus menghapus Instans Amazon Connect. Untuk informasi selengkapnya, lihat Menghapus instans Amazon Connect dalam Panduan Administrator Amazon Connect.
- Untuk menonaktifkan Amazon QuickSight, Anda harus berhenti berlangganan dari Amazon QuickSight. Untuk informasi selengkapnya, lihat Menutup Amazon QuickSight akun Anda di Panduan QuickSight Pengguna Amazon.

> **Note**
>
> Jika Anda menggunakan AWS IAM Identity Center dan sebelumnya telah menghubungkannya ke direktori Microsoft AD AWS Terkelola yang ingin Anda hapus, Anda harus terlebih dahulu mengubah sumber identitas sebelum dapat menghapusnya. Untuk informasi selengkapnya, lihat Mengubah sumber identitas Anda di Panduan Pengguna Pusat Identitas IAM.

3. Di panel navigasi, pilih Direktori.
4. Pilih hanya direktori yang akan dihapus dan klik Hapus. Ini akan memerlukan beberapa menit agar direktori dihapus. Ketika direktori telah dihapus, itu akan dihapus dari daftar direktori Anda.

Ganti nama situs direktori Anda

Anda dapat mengganti nama situs default direktori Microsoft AD yang Dikelola AWS sehingga cocok dengan nama situs Microsoft Active Directory (AD) yang ada. Ini membuat Microsoft AD yang Dikelola AWS lebih cepat untuk menemukan dan mengautentikasi pengguna AD yang ada di direktori on-premise Anda. Hasilnya adalah pengalaman yang lebih baik ketika pengguna masuk ke sumber daya AWS seperti instans Amazon EC2 dan Amazon RDS for SQL Server yang telah Anda gabungkan ke direktori Microsoft AD yang Dikelola AWS Anda.

Untuk melakukan itu, Anda harus masuk dengan akun Admin atau dengan akun yang merupakan anggota dari grup Administrator Situs dan Layanan yang Didelegasikan AWS. Untuk informasi selengkapnya tentang grup ini, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.

Untuk manfaat tambahan dari mengubah nama situs Anda dalam kaitannya dengan kepercayaan, lihat Domain Locator di Kepercayaan Forest di situs web Microsoft.

Untuk mengganti nama situs Microsoft AD yang Dikelola AWS

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Temukan instans Amazon EC2 yang digabungkan ke direktori Microsoft AD yang Dikelola AWS Anda. Pilih instans, lalu pilih Hubungkan.
3. Di jendela Pengelola Server, pilih Alat. Lalu pilih Situs dan Layanan Direktori Aktif.
4. Di panel sebelah kiri, perluas folder Situs, klik kanan nama situs (default adalah Default-Situs-Nama), lalu pilih Mengubah nama.
5. Ketik nama situs baru, dan kemudian pilih Masukkan.

Snapshot atau pulihkan direktori Anda

AWS Directory Servicemenyediakan snapshot harian otomatis dan kemampuan untuk mengambil snapshot manual data untuk Direktori Aktif AWS Microsoft AD Terkelola Anda. Snapshot ini dapat digunakan untuk melakukan point-in-time restore untuk Active Directory Anda. Anda dibatasi hingga lima snapshot manual untuk setiap Direktori Aktif Microsoft AD yang AWS Dikelola. Jika Anda telah mencapai batas ini, Anda harus menghapus salah satu snapshot manual yang ada sebelum Anda dapat membuat yang lain. Anda tidak dapat mengambil snapshot dari direktori AD Connector.

> **Note**
>
> Snapshot adalah fitur global dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus dilakukan di Region primer. Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Topik

- Membuat snapshot dari direktori Anda
- Memulihkan direktori Anda dari snapshot
- Menghapus snapshot

Membuat snapshot dari direktori Anda

Snapshot dapat digunakan untuk memulihkan direktori Anda ke apa itu pada titik waktu yang snapshot diambil. Untuk membuat snapshot manual dari direktori Anda, lakukan langkah-langkah berikut.

> **Note**
>
> Anda dibatasi hingga 5 snapshot manual untuk setiap direktori. Jika Anda telah mencapai batas ini, Anda harus menghapus salah satu snapshot manual yang ada sebelum Anda dapat membuat yang lain.

Untuk membuat snapshot manual

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Membuat snapshot.
5. Pada kotak dialog Membuat snapshot direktori, berikan nama untuk snapshot, jika diinginkan. Ketika siap, pilih Buat.

Tergantung pada ukuran direktori Anda, mungkin diperlukan beberapa menit untuk membuat snapshot. Ketika snapshot siap, nilai Status akan berubah menjadi `Completed`.

Memulihkan direktori Anda dari snapshot

Memulihkan direktori dari snapshot setara dengan memindahkan direktori kembali ke waktu dulu. Direktori snapshot unik untuk direktori tempat mereka dibuat. Snapshot hanya dapat dipulihkan ke direktori dari mana ia dibuat. Selain itu, usia maksimum yang didukung dari snapshot manual adalah 180 hari. Untuk informasi selengkapnya, lihat Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif di situs web Microsoft.

> **Warning**
>
> Kami rekomendasikan Anda menghubungi Pusat AWS Support sebelum pemulihan snapshot apa pun; kami mungkin dapat membantu Anda menghindari kebutuhan untuk melakukan pemulihan snapshot. Setiap pemulihan dari snapshot dapat mengakibatkan kehilangan data karena mereka adalah titik waktu. Penting untuk Anda memahami bahwa semua server DC dan DNS yang terasosiasi dengan direktori akan offline sampai operasi pemulihan telah selesai.

Untuk memulihkan direktori Anda dari snapshot, lakukan langkah-langkah berikut.

Untuk memulihkan direktori dari snapshot

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih snapshot dalam daftar, pilih Tindakan, dan kemudian pilih Memulihkan snapshot.
5. Tinjau informasi di kotak dialog Memulihkan snapshot direktori, dan pilih Pemulihan.

Untuk direktori Microsoft AD yang Dikelola AWS, diperlukan dua sampai tiga jam untuk memulihkan direktori. Ketika berhasil dipulihkan, nilai Status direktori berubah menjadi `Active`. Setiap perubahan yang dibuat ke direktori setelah tanggal snapshot akan ditimpa.

Menghapus snapshot

Untuk menghapus snapshot

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Hapus snapshot.
5. Verifikasi bahwa Anda ingin menghapus snapshot tersebut, lalu pilih Hapus.

Tingkatkan Direktori Aktif Microsoft AD AWS Terkelola

Anda dapat memutakhirkan Direktori Aktif Microsoft AD AWS Terkelola edisi Standar ke edisi Enterprise dengan menghubungi AWS Support. Untuk informasi selengkapnya, lihat Membuat kasus dukungan dan manajemen kasus di PanduanAWS Support Pengguna.

Ada beberapa batasan yang harus diperhatikan saat memutakhirkan Direktori Aktif Microsoft AD AWS Terkelola Anda. File tersebut adalah:

- Upgrade akan dikenakan biaya tambahan. Lihat AWS Directory Service Harga untuk informasi lebih lanjut.
- Setelah Active Directory Anda ditingkatkan, itu tidak dapat dikembalikan ke edisi sebelumnya.
- Snapshot sebelumnya tidak dapat digunakan untuk memulihkan Direktori Aktif setelah ditingkatkan.
- Upgrade terjadi pada tanggal dan waktu yang dijadwalkan yang disepakati. AWS SupportPeningkatan terjadi antara Senin hingga Jumat, 9 pagi - 5 sore Waktu Standar Pasifik.
- Proses upgrade membutuhkan empat hingga lima jam.
- Selama proses pemutakhiran, pengontrol domain Direktori Aktif Microsoft AD AWS Terkelola Anda ditingkatkan satu per satu. Hal ini dapat berdampak negatif pada kinerja Anda dan dapat menyebabkan downtime selama jendela pemeliharaan Anda.
- Jika aplikasi Anda menggunakan nama host atau alamat IP pengontrol domain alih-alih nama domain Active Directory Anda, aplikasi ini perlu diperbarui.
- Jika Anda menggunakan LDAPS (Lightweight Directory Access Protocol over SSL), pengontrol domain akan memerlukan sertifikat baru.

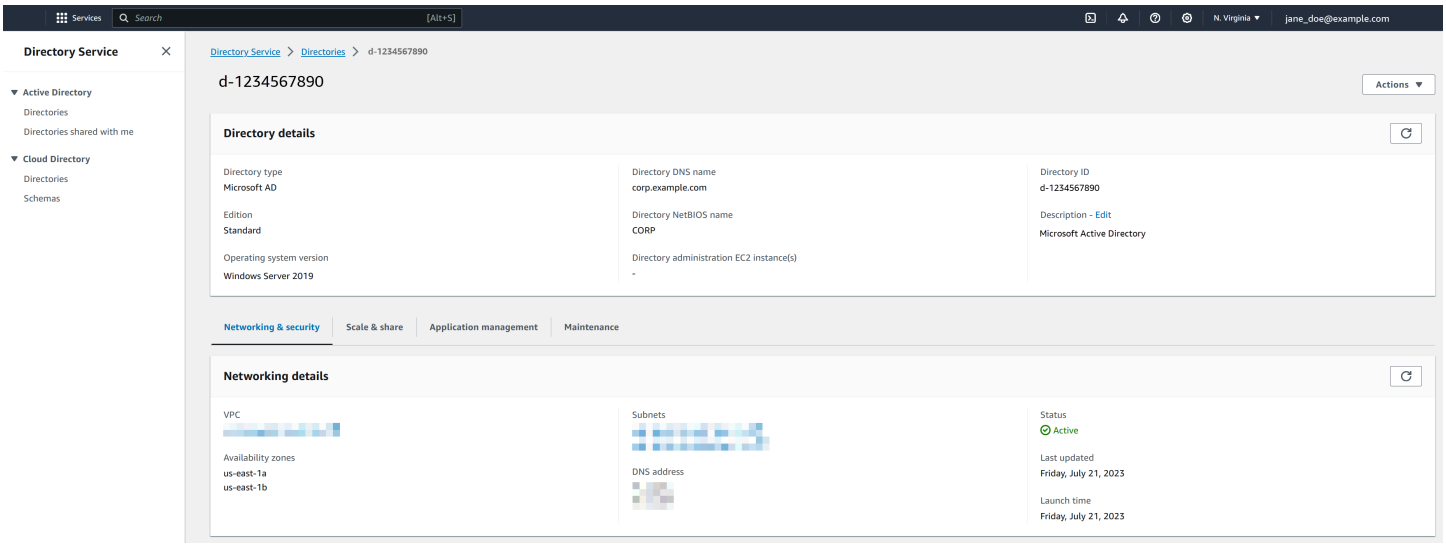
Melihat informasi direktori

Anda dapat melihat informasi detail tentang direktori.

Untuk melihat informasi direktori terperinci.

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori.
2. Klik tautan ID direktori untuk direktori Anda. Informasi tentang direktori ditampilkan dalam halaman Detail direktori.

Untuk informasi selengkapnya tentang bidang Status, lihat Memahami status direktori Anda.



Berikan akses ke pengguna dan grup sumber daya AWS

AWS Directory Service menyediakan kemampuan untuk memberikan pengguna direktori dan grup akses ke AWS layanan dan sumber daya, seperti akses ke konsol Amazon EC2. Mirip dengan memberikan akses kepada pengguna IAM untuk mengelola direktori seperti yang dijelaskan dalamKebijakan berbasis identitas (kebijakan IAM), agar pengguna di direktori Anda memiliki akses ke AWS sumber daya lain, seperti Amazon EC2, Anda harus menetapkan peran dan kebijakan IAM kepada pengguna dan grup tersebut. Untuk informasi selengkapnya, lihat peran IAM dalam Panduan Pengguna IAM.

Untuk informasi tentang cara memberi pengguna akses ke AWS Management Console, lihatMengaktifkan akses ke AWS Management Console dengan kredensial AD.

Topik

- Membuat peran baru
- Mengedit hubungan kepercayaan untuk peran yang ada
- Menetapkan pengguna atau grup ke peran yang ada
- Melihat pengguna dan grup yang ditetapkan ke peran
- Menghapus pengguna atau grup dari peran
- Menggunakan kebijakan yang dikelola AWS dengan AWS Directory Service

Membuat peran baru

Jika Anda perlu membuat peran IAM baru untuk digunakan AWS Directory Service, Anda harus membuatnya menggunakan konsol IAM. Setelah peran dibuat, Anda harus mengatur hubungan kepercayaan dengan peran itu sebelum Anda dapat melihat peran itu di AWS Directory Service konsol. Untuk informasi selengkapnya, lihat Mengedit hubungan kepercayaan untuk peran yang ada.

> **Note**
>
> Pengguna yang melakukan tugas ini harus memiliki izin untuk melakukan tindakan IAM berikut. Untuk informasi selengkapnya, lihat Kebijakan berbasis identitas (kebijakan IAM).
>
> - saya: PassRole
> - saya: GetRole
> - saya: CreateRole
> - saya: PutRolePolicy

Untuk membuat peran baru di konsol IAM

1. Di panel navigasi konsol IAM, pilih Peran. Untuk informasi selengkapnya, lihat Membuat Peran (AWS Management Console) dalam Panduan Pengguna IAM.
2. Pilih Buat peran.
3. Di bawah Pilih layanan yang akan menggunakan peran ini, pilih Directory Service, lalu pilih Berikutnya.
4. Pilih kotak centang di samping kebijakan (misalnya, AmazonEC2 FullAccess) yang ingin Anda terapkan ke pengguna direktori, lalu pilih Berikutnya.
5. Jika perlu, tambahkan tanda ke peran, lalu pilih Selanjutnya.

6. Berikan Nama peran dan opsional Deskripsi, lalu pilih Buat peran.

Contoh: Buat peran untuk mengaktifkan AWS Management Console akses

Daftar periksa berikut memberikan contoh tugas yang harus Anda selesaikan untuk membuat peran baru yang akan memberikan pengguna direktori tertentu akses ke konsol Amazon EC2.

1. Buat peran dengan konsol IAM menggunakan prosedur di atas. Saat diminta untuk kebijakan, pilih FullAccessAmazonec2.
2. Gunakan langkah-langkah di Mengedit hubungan kepercayaan untuk peran yang ada untuk mengedit peran yang baru saja Anda buat, dan kemudian tambahkan informasi hubungan kepercayaan yang diperlukan ke dokumen kebijakan. Langkah ini diperlukan agar peran terlihat segera setelah Anda mengaktifkan akses ke AWS Management Console langkah berikutnya.
3. Ikuti langkah-langkah di Mengaktifkan akses ke AWS Management Console dengan kredensial AD untuk mengkonfigurasi akses umum ke AWS Management Console.
4. Ikuti langkah-langkah di Menetapkan pengguna atau grup ke peran yang ada untuk menambahkan pengguna yang membutuhkan akses penuh ke sumber daya EC2 untuk peran baru.

Mengedit hubungan kepercayaan untuk peran yang ada

Anda dapat menetapkan peran IAM yang ada untuk AWS Directory Service pengguna dan grup Anda. Untuk melakukan ini, bagaimanapun, peran harus memiliki hubungan kepercayaan dengan AWS Directory Service. Saat Anda menggunakan AWS Directory Service untuk membuat peran menggunakan prosedur diMembuat peran baru, hubungan kepercayaan ini diatur secara otomatis. Anda hanya perlu membangun hubungan kepercayaan ini untuk IAM role yang tidak dibuat oleh AWS Directory Service.

Untuk membangun hubungan kepercayaan untuk peran yang ada untuk AWS Directory Service

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, di bawah Manajemen akses, pilih Peran.

   Konsol tersebut menampilkan peran di akun Anda.
3. Pilih nama peran yang ingin Anda ubah, dan sekali di halaman peran, pilih tab Trust relationship.
4. Pilih Edit kebijakan kepercayaan.
5. Di bawah Edit kebijakan kepercayaan, tempel yang berikut ini, lalu pilih Perbarui kebijakan.

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

Anda juga dapat memperbarui dokumen kebijakan ini menggunakan AWS CLI. Untuk informasi selengkapnya, lihat perbarui kepercayaan di Referensi Perintah.AWS CLI

Menetapkan pengguna atau grup ke peran yang ada

Anda dapat menetapkan peran IAM yang ada ke AWS Directory Service pengguna atau grup. Untuk melakukan ini, pastikan Anda telah menyelesaikan yang berikut ini.

Prasyarat

- Buat iklan Microsoft yang AWS Dikelola.
- Buat pengguna atau buat grup.
- Buat peran yang memiliki hubungan kepercayaan dengan AWS Directory Service. Anda dapat mengedit hubungan kepercayaan untuk peran yang ada.

> **Note**
>
> Akses untuk pengguna dalam grup nested dalam direktori Anda tidak didukung. Anggota grup induk memiliki akses konsol, tetapi anggota grup anak tidak.

Untuk menetapkan IAM role yang sudah ada ke pengguna atau grup .

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori.

2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin membuat tugas Anda, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
4. Gulir ke bawah ke AWS Management Consolebagian, pilih Tindakan dan Aktifkan.
5. Di bawah bagian Akses konsol delegasi, pilih nama peran IAM untuk peran IAM yang ada yang ingin Anda tetapkan kepada pengguna.
6. Pada halaman Peran yang dipilih, di bawah Mengelola pengguna dan grup untuk peran ini, pilih Tambahkan.
7. Pada halaman Menambahkan pengguna dan grup ke peran, di bawah Pilih Forest Direktori Aktif, pilih salah satu forest Microsoft AD yang Dikelola AWS (forest ini) atau forest on-premise (forest terpercaya), mana saja yang berisi di mana akun yang memerlukan akses ke AWS Management Console. Untuk informasi selengkapnya tentang cara mengatur forest terpercaya, lihat Tutorial: Buat hubungan kepercayaan antara Microsoft AD yang AWS Dikelola dan domain Direktori Aktif yang dikelola sendiri.
8. Di bawah Tentukan pengguna atau grup mana yang akan ditambahkan, pilih salah satu Temukan dengan pengguna atau Temukan dengan grup, dan kemudian ketik nama pengguna atau grup. Dalam daftar kecocokan yang mungkin, pilih pengguna atau grup yang ingin Anda tambahkan.
9. Pilih Tambahkan untuk menyelesaikan penetapan pengguna dan grup ke peran.

Melihat pengguna dan grup yang ditetapkan ke peran

Untuk melihat pengguna dan grup yang ditetapkan ke peran, lakukan langkah-langkah berikut.

Prasyarat

- Tetapkan pengguna atau grup Anda ke peran yang ada.

Untuk melihat pengguna dan grup yang ditetapkan ke peran

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori.

2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin melihat tugas Anda, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian Akses Konsol Delegasi, pilih peran IAM yang ingin Anda lihat.
5. Pada halaman Peran yang dipilih, di bagian Kelola pengguna dan grup untuk peran ini, Anda dapat melihat pengguna dan grup yang ditetapkan ke peran tersebut.

Menghapus pengguna atau grup dari peran

Untuk menghapus pengguna atau grup dari peran, lakukan langkah-langkah berikut.

Untuk menghapus pengguna atau grup dari peran

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menghapus tugas Anda, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian AWS Management Console, pilih peran yang ingin Anda lihat.
5. Pada halaman Peran yang dipilih, di bawah Mengelola pengguna dan grup untuk peran ini, pilih pengguna atau grup untuk menghapus peran dan pilih Hapus. Peran dihapus dari pengguna dan grup tertentu, namun peran tersebut tidak dihapus dari akun Anda.

Menggunakan kebijakan yang dikelola AWS dengan AWS Directory Service

AWS Directory Service menyediakan kebijakan yang dikelola AWS untuk memberikan pengguna direktori dan grup Anda akses ke layanan dan sumber daya AWS, seperti akses ke konsol Amazon EC2. Anda harus masuk ke AWS Management Console sebelum Anda dapat melihat kebijakan ini.

- Akses hanya baca
- Akses pengguna kuat
- AWS Directory Serviceakses penuh
- AWS Directory Serviceakses hanya baca
- Akses penuh Amazon Cloud Directory
- Akses hanya baca Amazon Cloud Directory
- Akses penuh Amazon EC2
- Akses hanya baca Amazon EC2
- Akses penuh Amazon VPC
- Akses hanya baca Amazon VPC
- Akses penuh Amazon RDS
- Akses hanya baca Amazon RDS
- Akses penuh Amazon DynamoDB
- Akses hanya baca Amazon DynamoDB
- Akses penuh Amazon S3
- Akses hanya baca Amazon S3
- AWS CloudTrailakses penuh
- AWS CloudTrailakses hanya baca
- Akses penuh Amazon CloudWatch
- Akses hanya baca Amazon CloudWatch
- Akses penuh Amazon CloudWatch Logs
- Akses hanya baca Amazon CloudWatch Logs

Untuk informasi selengkapnya tentang cara membuat kebijakan Anda sendiri, lihat Contoh kebijakan untuk administrasi sumber daya AWS di Panduan Pengguna IAM.

Aktifkan akses ke AWS aplikasi dan layanan

Pengguna dapat mengotorisasi Microsoft AD yang AWS Dikelola untuk memberikan AWS aplikasi dan layanan, seperti Amazon WorkSpaces, akses ke aplikasi AndaActive Directory. AWS Aplikasi dan layanan berikut dapat diaktifkan atau dinonaktifkan untuk bekerja dengan Microsoft AD yang AWS Dikelola.

AWS aplikasi/layanan	Informasi selengkapnya…
Amazon Chime	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Chime.
Amazon Connect	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Connect.
Amazon FSx for Windows File Server	Untuk informasi selengkapnya, lihat Menggunakan Amazon FSx dengan AWS Directory Service untuk Microsoft Active Directory.
Amazon QuickSight	Untuk informasi selengkapnya, lihat Panduan QuickSight Pengguna Amazon.
Amazon Relational Database Service	Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon RDS.
Amazon WorkDocs	Untuk informasi selengkapnya, lihat Panduan WorkDocs Administrasi Amazon.
Amazon WorkMail	Untuk informasi selengkapnya, lihat Panduan WorkMail Administrator Amazon.
Amazon WorkSpaces	Anda dapat membuat Simple AD, AWS Managed Microsoft AD, atau AD Connector langsung dari WorkSpaces. Cukup luncurkan Pengaturan Advanced saat membuat Workspace Anda.

AWS aplikasi/layanan	Informasi selengkapnya…
	Untuk informasi selengkapnya, lihat Panduan WorkSpaces Administrasi Amazon.
AWS Client VPN	Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Client VPN.
AWS IAM Identity Center	Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS IAM Identity Center.
AWS License Manager	Untuk informasi selengkapnya, lihat Panduan Pengguna License Manager.
AWS Management Console	Untuk informasi selengkapnya, lihat Mengaktifkan akses ke AWS Management Console dengan kredensial AD.
AWS Private Certificate Authority	Untuk informasi selengkapnya, lihat AWS Private CA Konektor untuk Active Directory.
AWS Transfer Family	Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Transfer Family.

Setelah diaktifkan, Anda mengelola akses ke direktori Anda di konsol dari aplikasi atau layanan yang ingin Anda berikan akses ke direktori Anda. Untuk menemukan tautan AWS aplikasi dan layanan yang dijelaskan di atas di AWS Directory Service konsol, lakukan langkah-langkah berikut.

Untuk menampilkan aplikasi dan layanan untuk direktori

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Tinjau daftar di bawah bagian aplikasi & layanan AWS .

Untuk informasi selengkapnya tentang cara mengotorisasi atau membatalkan otorisasi AWS aplikasi dan layanan yang digunakan AWS Directory Service, lihat. Otorisasi untuk AWS aplikasi dan layanan menggunakan AWS Directory Service

Topik

Membuat URL akses

URL akses digunakan dengan AWS aplikasi dan layanan, seperti Amazon WorkDocs, untuk mencapai halaman login yang terkait dengan direktori Anda. URL harus unik secara global. Anda dapat membuat URL akses untuk direktori Anda dengan melakukan langkah-langkah berikut.

Warning

Setelah Anda membuat URL akses aplikasi untuk direktori ini, itu tidak dapat diubah. Setelah URL akses dibuat, tidak dapat digunakan oleh orang lain. Jika Anda menghapus direktori Anda, URL akses juga dihapus dan kemudian dapat digunakan oleh akun lain.

Note

URL akses hanya dapat dikonfigurasi dari wilayah utama saat menggunakan direktori multi-wilayah.

Untuk membuat URL akses

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Wilayah yang ditampilkan di bawah replikasi Multi-Region, pilih Wilayah Utama dan kemudian pilih tab Manajemen aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bagian URL akses aplikasi, jika URL akses belum ditetapkan ke direktori, tombol Buat ditampilkan. Masukkan alias direktori dan pilih Buat. Jika error Entitas Sudah Ada dikembalikan, alias direktori tertentu telah dialokasikan. Pilih alias lain dan ulangi prosedur ini.

URL akses Anda ditampilkan dalam format *<alias>*.awsapps.com. Secara default, URL ini akan membawa Anda ke halaman masuk untuk Amazon WorkDocs.

Sign-on tunggal

AWS Directory Servicemenyediakan kemampuan untuk memungkinkan pengguna Anda mengakses Amazon WorkDocs dari komputer yang bergabung ke direktori tanpa harus memasukkan kredensialnya secara terpisah.

Sebelum mengaktifkan sing-on tunggal, Anda perlu mengambil langkah tambahan agar peramban web pengguna dapat mendukung sign-on tunggal. Pengguna mungkin perlu memodifikasi pengaturan peramban web mereka untuk mengaktifkan sign-on tunggal.

> **Note**
>
> Sign-on tunggal hanya bekerja bila digunakan pada komputer yang digabungkan ke direktori AWS Directory Service. Ini tidak dapat digunakan pada komputer yang tidak bergabung ke direktori.

Jika direktori Anda adalah direktori AD Connector dan akun layanan AD Connector tidak memiliki izin untuk menambahkan atau menghapus atribut nama utama layanannya, maka untuk Langkah 5 dan 6 di bawah ini, Anda memiliki dua pilihan:

1. Anda dapat melanjutkan dan akan diminta untuk nama pengguna dan kata sandi untuk pengguna direktori yang memiliki izin ini untuk menambah atau menghapus atribut nama utama layanan pada akun layanan AD Connector. Kredensial ini hanya digunakan untuk mengaktifkan sign-on tunggal dan tidak disimpan oleh layanan. Izin akun layanan AD Connector tidak berubah.
2. Anda dapat mendelegasikan izin untuk mengizinkan akun layanan AD Connector menambah atau menghapus atribut nama utama layanan itu sendiri, Anda dapat menjalankan PowerShell perintah di bawah ini dari komputer yang bergabung dengan domain menggunakan akun yang memiliki izin untuk mengubah izin pada akun layanan AD Connector. Perintah di bawah ini akan memberikan akun layanan AD Connector kemampuan untuk menambah dan menghapus atribut nama utama layanan hanya untuk dirinya sendiri.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
```

```
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Untuk mengaktifkan atau menonaktifkan sistem masuk tunggal dengan Amazon WorkDocs

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bagian URL akses aplikasi, pilih Aktifkan untuk mengaktifkan sistem masuk tunggal untuk Amazon. WorkDocs

   Jika Anda tidak melihat tombol Aktifkan, Anda mungkin harus terlebih dahulu membuat URL Akses sebelum opsi ini akan ditampilkan. Untuk informasi selengkapnya tentang cara membuat URL akses, lihat Membuat URL akses.
5. Di kotak dialog Aktifkan Sign-On Tunggal untuk direktori ini,, pilih Aktifkan. Sign-on tunggal diaktifkan untuk direktori.
6. Jika nanti Anda ingin menonaktifkan sistem masuk tunggal dengan Amazon WorkDocs, pilih Nonaktifkan, lalu di kotak dialog Nonaktifkan Single Sign-On untuk direktori ini, pilih Nonaktifkan lagi.

Topik

- Sign-on tunggal untuk IE dan Chrome
- Sign-on tunggal untuk Firefox

Sign-on tunggal untuk IE dan Chrome

Untuk mengizinkan peramban Microsoft Internet Explorer (IE) dan Google Chrome untuk mendukung sign-on tunggal, tugas berikut harus dilakukan pada komputer klien:

- Tambahkan URL akses Anda (misalnya, https://*<alias>*.awsapps.com) ke daftar situs yang disetujui untuk sign-on tunggal.
- Aktifkan skrip aktif (JavaScript).
- Izinkan masuk otomatis.
- Aktifkan autentikasi terintegrasi.

Anda atau pengguna Anda dapat melakukan tugas-tugas ini secara manual, atau Anda dapat mengubah pengaturan ini menggunakan pengaturan Kebijakan Grup.

Topik

- Pembaruan manual untuk sign-on tunggal pada Windows
- Pembaruan manual untuk sign-on tunggal pada OS X
- Pengaturan kebijakan grup untuk sign-on tunggal

Pembaruan manual untuk sign-on tunggal pada Windows

Untuk mengaktifkan sign-on tunggal secara manual pada komputer Windows, lakukan langkah-langkah berikut pada komputer klien. Beberapa pengaturan ini mungkin sudah diatur dengan benar.

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome secara manual di Windows

1. Untuk membuka kotak dialog Properti internet, pilih menu Start, ketik `Internet Options` di kotak pencarian, lalu pilih Opsi Internet.
2. Tambahkan URL akses Anda ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
   a. Di kotak dialog Properti internet, pilih tab Keamanan.
   b. Pilih Intranet lokal dan pilih Situs.

c. Di kotak dialog Intranet lokal, pilih Advanced.

d. Tambahkan URL akses Anda ke daftar situs web dan pilih tutup.

e. Di dialog box Intranet lokal, pilih OK.

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:

a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.

b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Penulisan dan pilih Aktifkan di bawah Penulisan aktif.

c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.

4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:

a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.

b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Autentikasi Pengguna dan pilih Masuk otomatis hanya di zona Intranet di bawah Masuk.

c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.

d. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.

5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:

a. Di kotak dialog Properti internet, pilih tab Advanced.

b. Gulir ke bawah ke Keamanan dan pilih Mengaktifkan Autentikasi Windows Terintegrasi.

c. Di kotak dialog Properti Internet, pilih OK.

6. Tutup dan buka kembali peramban Anda agar perubahan ini berlaku.

Pembaruan manual untuk sign-on tunggal pada OS X

Untuk mengaktifkan sign-on tunggal secara manual untuk Chrome pada OS X, lakukan langkah-langkah berikut pada komputer klien. Anda memerlukan hak administrator di komputer Anda untuk menyelesaikan langkah-langkah ini.

Cara mengaktifkan sign-on tunggal untuk Chrome di OS X secara manual

1. Tambahkan URL akses Anda ke AuthServerAllowlistkebijakan dengan menjalankan perintah berikut:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Buka Preferensi Sistem, buka panel Profil, dan hapus profil `Chrome Kerberos Configuration`.
3. Mulai ulang Chrome dan buka chrome://policy di Chrome untuk mengonfirmasi bahwa pengaturan baru sudah terpasang.

Pengaturan kebijakan grup untuk sign-on tunggal

Administrator domain dapat menerapkan pengaturan Kebijakan Grup untuk membuat perubahan sign-on tunggal pada komputer klien yang digabungkan ke domain.

> **Note**
>
> Jika Anda mengelola browser web Chrome di komputer di domain Anda dengan kebijakan Chrome, Anda harus menambahkan URL akses ke AuthServerAllowlistkebijakan. Untuk informasi selengkapnya tentang mengatur kebijakan Chrome, kunjungi Pengaturan Kebijakan di Chrome.

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome menggunakan pengaturan Kebijakan Grup

1. Membuat objek Kebijakan Grup baru dengan melakukan langkah-langkah berikut:
   a. Buka alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, lalu pilih Objek Kebijakan Grup.
   b. Dari menu utama, pilih Tindakan dan pilih Baru.
   c. Di kotak dialog GPO baru, masukkan nama deskriptif untuk objek Kebijakan Grup, seperti `IAM Identity Center Policy`, dan biarkan Sumber Starter GPO diatur ke (tidak ada). Klik OK.
2. Tambahkan URL akses ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:

a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.

b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.

c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.

d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

   Aksi

   ```
   Update
   ```

   Sarang

   ```
   HKEY_CURRENT_USER
   ```

   Jalan

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   \ZoneMap\Domains\awsapps.com\<alias>
   ```

   Nilai untuk *<alias>* berasal dari URL akses Anda. Jika URL akses Anda adalah `https://examplecorp.awsapps.com`, alias adalah `examplecorp`, dan kunci registri akan menjadi `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

   Nama nilai

   ```
   https
   ```

   Jenis nilai

   ```
   REG_DWORD
   ```

   Data nilai

   ```
   1
   ```

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:

   a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.

b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.

c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Izinkan penulisan aktif dan pilih Edit.

d. Di kotak dialog Izinkan penulisan aktif, masukkan pengaturan berikut dan pilih OK:

- Pilih tombol radio Diaktifkan.
- Di bawah Opsi atur Izinkan penulisan aktif ke Aktifkan.

4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:

a. Pada alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan SSO Anda, lalu pilih Edit.

b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.

c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Opsi masuk dan pilih Edit.

d. Di kotak dialog Opsi masuk, masukkan pengaturan berikut dan pilih OK:

- Pilih tombol radio Diaktifkan.
- Di bawah Opsi atur Opsi masuk ke Masuk otomatis hanya di zona Intranet.

5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:

a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.

b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.

c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.

d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

Aksi

```
Update
```

Sarang

```
HKEY_CURRENT_USER
```

Jalan

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Nama nilai

```
EnableNegotiate
```

Jenis nilai

```
REG_DWORD
```

Data nilai

```
1
```

6. Tutup jendela Editor Pengelolaan Kebijakan Grup jika masih terbuka.
7. Tetapkan kebijakan baru ke domain Anda dengan mengikuti langkah-langkah berikut:
   a. Di pohon Pengelolaan Kebijakan Grup, buka menu konteks (klik kanan) untuk domain Anda, lalu pilih Menautkan GPO yang Ada.
   b. Dalam daftar Objek Kebijakan Grup, pilih kebijakan Pusat Identitas IAM Anda dan pilih OK.

Perubahan ini akan berlaku setelah pembaruan Kebijakan Grup berikutnya pada klien, atau waktu berikutnya pengguna masuk.

Sign-on tunggal untuk Firefox

Untuk mengizinkan peramban Mozilla Firefox untuk mendukung sign-on tunggal, tambahkan URL akses Anda (misalnya, https://*<alias>*.awsapps.com) ke daftar situs yang disetujui untuk sign-on tunggal. Ini bisa dilakukan secara manual, atau otomatis dengan skrip.

Topik

- Pembaruan manual untuk sign-on tunggal
- Pembaruan otomatis untuk sign-on tunggal

Pembaruan manual untuk sign-on tunggal

Untuk menambahkan URL akses Anda ke daftar situs yang disetujui di Firefox secara manual, lakukan langkah-langkah berikut pada komputer klien.

Untuk menambahkan URL akses Anda secara manual ke daftar situs yang disetujui di Firefox

1. Buka Firefox dan buka halaman `about:config`.
2. Buka preferensi `network.negotiate-auth.trusted-uris` dan tambahkan URL akses Anda ke daftar situs. Gunakan koma (,) untuk memisahkan beberapa entri.

Pembaruan otomatis untuk sign-on tunggal

Sebagai administrator domain, Anda dapat menggunakan skrip untuk menambahkan URL akses ke preferensi pengguna `network.negotiate-auth.trusted-uris` Firefox pada semua komputer di jaringan Anda. Untuk informasi selengkapnya, kunjungi https://support.mozilla.org/en-US/questions/939037.

Mengaktifkan akses ke AWS Management Console dengan kredensial AD

AWS Directory Service memungkinkan Anda untuk memberikan anggota direktori Anda akses ke AWS Management Console. Secara default, anggota direktori Anda tidak memiliki akses ke sumber daya AWS mana pun. Anda menetapkan IAM role untuk anggota direktori Anda untuk memberikan mereka akses ke berbagai layanan dan sumber daya AWS. IAM role menentukan layanan, sumber daya, dan tingkat akses yang dimiliki anggota direktori Anda.

Sebelum Anda dapat memberikan akses konsol ke anggota direktori Anda, direktori Anda harus memiliki URL akses. Untuk informasi selengkapnya tentang cara melihat detail direktori dan mendapatkan URL akses Anda, lihat Melihat informasi direktori. Untuk informasi selengkapnya tentang cara membuat URL akses, lihat Membuat URL akses.

Untuk informasi selengkapnya tentang cara membuat dan menetapkan IAM role untuk anggota direktori Anda, lihat Berikan akses ke pengguna dan grup sumber daya AWS.

Topik

- Aktifkan akses AWS Management Console
- Menonaktifkan akses AWS Management Console
- Mengatur lamanya sesi masuk

TerkaitAWSArtikel Blog Keamanan

- Cara mengaksesAWS Management ConsoleMenggunakanAWSMicrosoft AD yang Dikelola dan Kredensi On-premise Anda

> **Note**
>
> Akses ke AWS Management Console adalah fitur Regional dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Aktifkan akses AWS Management Console

Secara default, akses konsol tidak diaktifkan untuk direktori apapun. Untuk mengaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk mengaktifkan akses konsol

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengaktifkan akses ke AWS Management Console, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian AWS Management Console, pilih Aktifkan. Akses konsol sekarang diaktifkan untuk direktori Anda.

   Sebelum pengguna dapat masuk ke konsol tersebut dengan URL akses Anda, Anda harus terlebih dahulu menambahkan pengguna Anda ke peran. Untuk informasi umum tentang menetapkan pengguna ke IAM role, lihat Menetapkan pengguna atau grup ke peran yang ada. Setelah IAM role telah ditetapkan, pengguna kemudian dapat mengakses konsol tersebut menggunakan URL akses Anda. Misalnya, jika URL akses direktori Anda adalah example-corp.awsapps.com, URL untuk mengakses konsol tersebut adalah https://example-corp.awsapps.com/console/.

Menonaktifkan akses AWS Management Console

Untuk menonaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk menonaktifkan akses konsol

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menonaktifkan akses ke AWS Management Console, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian AWS Management Console, pilih Menonaktifkan. Akses konsol sekarang dinonaktifkan untuk direktori Anda.
5. Jika setiap IAM role telah ditetapkan untuk pengguna atau grup dalam direktori, tombol Nonaktifkan mungkin tidak tersedia. Dalam kasus ini, Anda harus menghapus semua penetapan IAM role untuk direktori sebelum melanjutkan, termasuk tugas untuk pengguna atau grup dalam direktori Anda yang telah dihapus, yang akan ditampilkan sebagai Pengguna Dihapus atau Grup Dihapus.

   Setelah semua penetapan IAM role dihapus, ulangi langkah-langkah di atas.

Mengatur lamanya sesi masuk

Secara default, pengguna memiliki waktu 1 jam untuk menggunakan sesi mereka setelah berhasil masuk ke konsol tersebut sebelum mereka keluar. Setelah itu, pengguna harus masuk lagi untuk memulai sesi 1 jam berikutnya sebelum keluar lagi. Anda dapat menggunakan prosedur berikut untuk mengubah lama waktu hingga 12 jam per sesi.

Untuk mengatur lamanya sesi masuk

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.

3. Pada halaman Detail direktori, lakukan salah satu hal berikut:

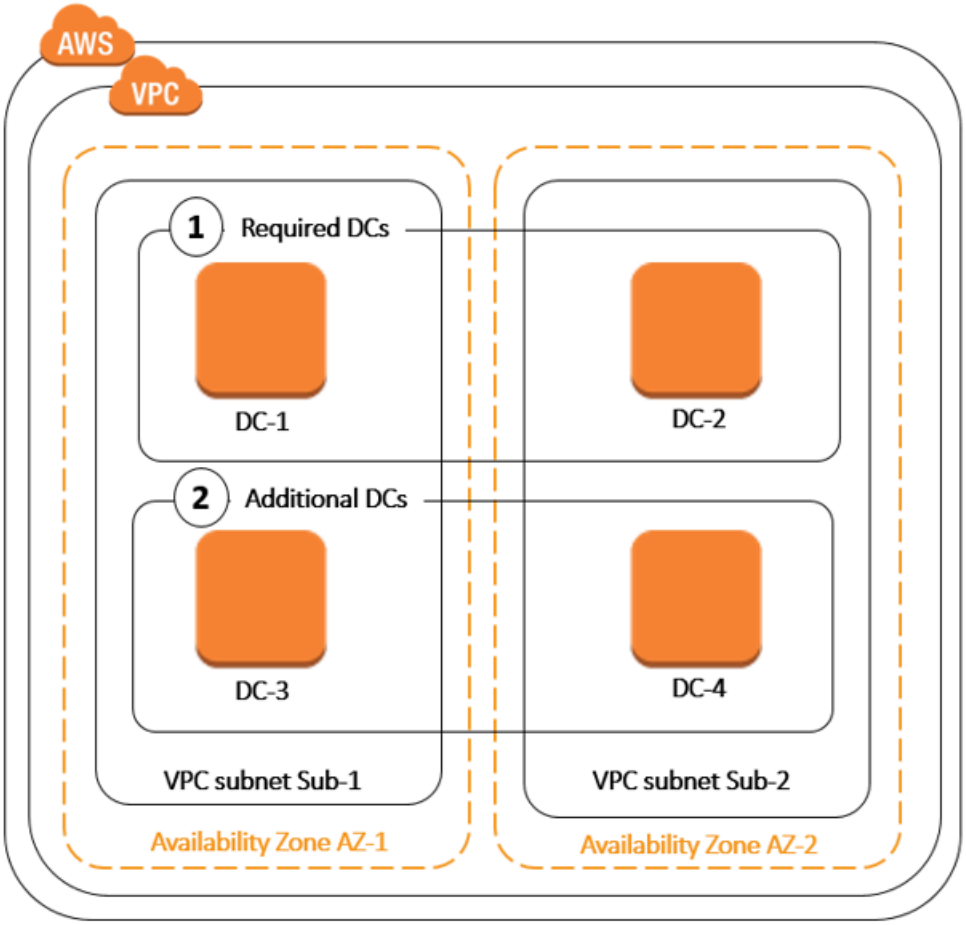
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin mengatur lamanya sesi, lalu pilih tab Pengelolaan Aplikasi. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Pengelolaan Aplikasi.
4. Di bawah bagian Aplikasi & layanan AWS, pilih Konsol Manajemen AWS.
5. Di kotak dialog Mengelola Akses ke Sumber Daya AWS, pilih Lanjutkan.
6. Di halamanMenetapkan pengguna dan grup ke IAM role, di bawah Atur lamanya sesi masuk, edit nilai bernomor, dan kemudian pilih Simpan.

Men-deploy pengendali domain tambahan

Men-deploy pengendali domain tambahan meningkatkan redundansi, yang di mana menghasilkan ketahanan yang lebih besar dan ketersediaan yang lebih tinggi. Hal ini juga meningkatkan performa direktori Anda dengan mendukung lebih banyak permintaan Direktori Aktif. Misalnya, Anda sekarang dapat menggunakan Microsoft AD yang AWS Dikelola untuk mendukung beberapa aplikasi.NET yang digunakan pada armada besar Amazon EC2 dan Amazon RDS for SQL Server.

Saat pertama kali membuat direktori, Microsoft AD AWS Terkelola akan menerapkan dua pengontrol domain di beberapa Availability Zone, yang diperlukan untuk tujuan ketersediaan tinggi. Kemudian, Anda dapat dengan mudah menerapkan pengontrol domain tambahan melalui AWS Directory Service konsol hanya dengan menentukan jumlah total pengontrol domain yang Anda inginkan. AWS Microsoft AD yang dikelola mendistribusikan pengontrol domain tambahan ke Availability Zones dan subnet Amazon VPC tempat direktori Anda berjalan.

Misalnya, dalam ilustrasi di bawah ini, DC-1 dan DC-2 mewakili dua pengendali domain yang awalnya dibuat dengan direktori Anda. AWS Directory Service Konsol mengacu pada pengontrol domain default ini sebagai Diperlukan. AWS Microsoft AD yang dikelola dengan sengaja menempatkan masing-masing pengontrol domain ini di Availability Zone terpisah selama proses pembuatan direktori. Kemudian, Anda mungkin memutuskan untuk menambahkan dua pengontrol domain lagi untuk membantu mendistribusikan beban autentikasi selama waktu masuk puncak. DC-3 dan DC-4 mewakili pengendali domain baru, yang di mana konsol tersebut sekarang mengacu sebagai Tambahan. Seperti sebelumnya, Microsoft AD yang AWS Dikelola kembali secara otomatis menempatkan pengontrol domain baru di Availability Zone yang berbeda untuk memastikan ketersediaan domain Anda yang tinggi.



Proses ini menghilangkan kebutuhan Anda untuk secara manual mengkonfigurasi direktori data replikasi, snapshot harian otomatis, atau pemantauan untuk pengendali domain tambahan. Juga lebih mudah bagi Anda untuk memigrasi dan menjalankan beban kerja yang terintegrasi dengan Direktori Aktif bermisi kritis di Cloud AWS tanpa harus men-deploy dan memelihara infrastruktur Direktori Aktif Anda sendiri. Anda juga dapat menerapkan atau menghapus pengontrol domain tambahan untuk AWS Microsoft AD yang Dikelola menggunakan API. UpdateNumberOfDomainControllers

> **Note**
>
> Pengontrol domain tambahan adalah fitur Regional dari Microsoft AD yang AWS Dikelola. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus diterapkan secara terpisah di setiap Region. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Menambah atau menghapus pengendali domain tambahan

Sebelum menambahkan atau menghapus pengontrol domain tambahan, berikut informasi selengkapnya tentang persyaratan pengontrol domain:

- Setelah men-deploy pengendali domain tambahan, Anda dapat mengurangi jumlah pengendali domain hingga dua, yang merupakan minimum yang diperlukan untuk toleransi kesalahan dan tujuan ketersediaan tinggi.
- Pengontrol domain yang dihapus akan dihapus dari daftar pengontrol domain tambahan. Pengontrol domain primer dan sekunder diperlukan dan tidak dapat dihapus.
- Jika Anda telah mengonfigurasi iklan Microsoft AWS Terkelola untuk mengaktifkan LDAPS, pengontrol domain tambahan apa pun yang Anda tambahkan juga akan mengaktifkan LDAPS secara otomatis. Untuk informasi selengkapnya, lihat Aktifkan LDAP atau LDAPS yang aman.

Gunakan prosedur berikut untuk men-deploy atau menghapus pengendali domain di direktori Microsoft AD yang Dikelola AWS Anda.

Untuk menambah atau menghapus pengendali domain tambahan

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi Multi-Region, pilih Region tempat Anda ingin menambahkan menghapus pengendali domain, lalu pilih tab Menskalakan & bagikan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Menskalakan & bagikan.
4. Di bagian Pengendali Domain, pilih Edit.
5. Tentukan jumlah pengendali domain untuk menambah atau menghapus dari direktori Anda, dan kemudian pilih Modifikasi.
6. Saat Microsoft AD AWS Terkelola menyelesaikan proses penerapan, semua pengontrol domain menampilkan status Aktif, dan subnet Availability Zone dan Amazon VPC yang ditetapkan akan muncul. Pengendali domain baru sama-sama didistribusikan di Availability Zone dan subnet di mana direktori Anda sudah di-deploy.

Artikel Blog AWS Keamanan Terkait

- Cara meningkatkan redundansi dan kinerja iklan AWS Microsoft Terkelola Anda AWS Directory Service dengan menambahkan pengontrol domain

Memigrasi pengguna dari Direktori Aktif ke Microsoft AD yang Dikelola AWS

Anda dapat menggunakan Active Directory Migration Toolkit (ADMT) bersama dengan Layanan Ekspor Kata Sandi (PES) untuk memigrasikan pengguna dari Direktori Aktif yang dikelola sendiri ke direktori AD AWS Microsoft Terkelola Anda. Ini memungkinkan Anda untuk memigrasi objek Active Directory dan kata sandi terenkripsi untuk pengguna Anda dengan lebih mudah.

Untuk instruksi detail, lihat Cara memigrasi domain on-premise Anda ke Microsoft AD yang Dikelola AWS menggunakan ADMT pada Blog Keamanan AWS.

Praktik terbaik untuk Microsoft AD yang AWS Dikelola

Berikut adalah beberapa saran dan pedoman yang harus Anda pertimbangkan untuk menghindari masalah dan mendapatkan hasil maksimal dari Microsoft AD yang AWS Dikelola.

Menyiapkan: Prasyarat

Pertimbangkan panduan ini sebelum membuat direktori Anda.

Verifikasikan Anda memiliki jenis direktori yang tepat

AWS Directory Service menyediakan berbagai cara untuk digunakan dengan AWS layanan lain. Anda dapat memilih directory service dengan fitur yang Anda butuhkan dengan biaya yang sesuai dengan anggaran Anda:

- AWS Directory Service untuk Microsoft Active Directory adalah pengelola yang kaya fitur yang dihosting di cloud. AWS AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memiliki lebih dari 5.000 pengguna dan memerlukan hubungan kepercayaan yang disiapkan antara direktori yang AWS dihosting dan direktori lokal Anda.
- AD Connector hanya menghubungkan lokal Active Directory Anda yang sudah ada. AWS AD Connector adalah pilihan terbaik Anda saat Anda ingin menggunakan direktori on-premise Anda yang sudah ada dengan layanan AWS .

- Simple AD adalah direktori berskala rendah dan berbiaya rendah dengan kompatibilitas dasarActive Directory. Ini mendukung 5.000 atau lebih sedikit pengguna, aplikasi yang kompatibel dengan Samba 4, dan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Untuk perbandingan AWS Directory Service opsi yang lebih rinci, lihatMana yang harus dipilih.

Pastikan VPC dan instans Anda dikonfigurasi dengan benar

Untuk terhubung ke, mengelola, dan menggunakan direktori Anda, Anda harus mengkonfigurasi VPC yang terkait direktori dengan benar. Lihat AWS Prasyarat Microsoft AD yang dikelola, Prasyarat AD Connector, atau Prasyarat Simple AD untuk informasi tentang persyaratan keamanan dan jaringan VPC.

Jika Anda menambahkan instans ke domain Anda, pastikan bahwa Anda memiliki konektivitas dan akses jarak jauh ke instans Anda seperti yang dijelaskan di Bergabunglah dengan instans Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola.

Ketahui batasan Anda

Pelajari tentang berbagai batasan untuk jenis direktori spesifik Anda. Penyimpanan yang tersedia dan ukuran agregat objek Anda adalah satu-satunya keterbatasan terkait jumlah objek yang dapat Anda simpan dalam direktori Anda. Lihat Kuota Microsoft AD yang Dikelola AWS, Kuota AD Connector, atau Kuota Simple AD untuk detail tentang direktori pilihan Anda.

Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan

AWS membuat grup keamanan dan melampirkannya ke antarmuka jaringan elastis pengontrol domain direktori Anda. Grup keamanan ini memblokir lalu lintas yang tidak perlu untuk pengendali domain dan memungkinkan lalu lintas yang diperlukan untuk komunikasi Direktori Aktif. AWS mengonfigurasi grup keamanan untuk membuka hanya port-port yang diperlukan untuk komunikasi Direktori Aktif. Dalam konfigurasi default, grup keamanan menerima lalu lintas ke port ini dari alamat IP apa pun. AWS melampirkan grup keamanan ke antarmuka pengontrol domain Anda yang dapat diakses dari dalam VPC yang di-peered atau diubah ukurannya. Antarmuka ini tidak dapat diakses dari internet bahkan jika Anda mengubah tabel perutean, mengubah koneksi jaringan ke VPC Anda, dan mengkonfigurasi layanan NAT Gateway. Dengan demikian, hanya instans dan komputer yang memiliki jalur jaringan ke VPC dapat mengakses direktori. Ini menyederhanakan pengaturan dengan menghilangkan persyaratan bagi Anda untuk mengkonfigurasi rentang alamat tertentu. Sebaliknya, Anda mengkonfigurasi rute dan grup keamanan ke VPC yang mengizinkan lalu lintas hanya dari instans dan komputer terpercaya.

Memodifikasi grup keamanan direktori

Jika Anda ingin meningkatkan keamanan dari grup keamanan direktori Anda, Anda dapat memodifikasi mereka untuk menerima lalu lintas dari daftar alamat IP yang lebih ketat. Misalnya, Anda dapat mengubah alamat diterima dari 0.0.0.0/0 ke kisaran CIDR yang spesifik untuk subnet tunggal atau komputer. Demikian pula, Anda dapat memilih untuk membatasi alamat tujuan yang di mana pengendali domain Anda bisa berkomunikasi. Hanya buat perubahan tersebut jika Anda sepenuhnya memahami cara kerja filter grup keamanan. Untuk informasi selengkapnya, lihat Grup Keamanan Amazon EC2 untuk instans Linux di Panduan Pengguna Amazon EC2. Perubahan yang tidak tepat dapat mengakibatkan hilangnya komunikasi ke komputer dan instance yang dituju. AWS merekomendasikan agar Anda tidak mencoba membuka port tambahan ke pengontrol domain karena ini mengurangi keamanan direktori Anda. Harap tinjau dengan seksama Model Tanggung Jawab Bersama AWS.

> **Warning**
>
> Hal itu mungkin secara teknis untuk Anda dapat mengasosiasikan grup keamanan direktori dengan instans EC2 lain yang Anda buat. Namun, AWS merekomendasikan untuk tidak melakukan praktik ini. AWS mungkin memiliki alasan untuk memodifikasi grup keamanan tanpa pemberitahuan untuk mengatasi kebutuhan fungsional atau keamanan direktori terkelola. Perubahan tersebut mempengaruhi setiap instans yang Anda asosiasikan dengan grup keamanan direktori. Selain itu, mengasosiasikan grup keamanan direktori dengan instans EC2 Anda dapat menciptakan risiko keamanan potensial untuk instans EC2 Anda. Grup keamanan direktori menerima lalu lintas pada port-port Direktori Aktif yang diperlukan dari alamat IP. Jika Anda mengasosiasikan grup keamanan ini dengan instans EC2 yang memiliki alamat IP publik yang terpasang ke internet, maka setiap komputer di internet dapat berkomunikasi dengan Anda instans EC2 pada port-port yang terbuka.

Pengaturan: Membuat direktori Anda

Berikut adalah beberapa saran untuk dipertimbangkan saat Anda membuat direktori Anda.

Ingat ID dan kata sandi administrator Anda

Saat mengatur direktori Anda, Anda memberikan kata sandi untuk akun administrator. ID akun tersebut adalah Admin untuk Microsoft AD yang AWS Dikelola. Ingat kata sandi yang Anda buat untuk akun ini; jika tidak, Anda tidak akan dapat menambahkan objek ke direktori Anda.

Buat set opsi DHCP

Kami menyarankan Anda membuat opsi DHCP yang ditetapkan untuk AWS Directory Service direktori Anda dan menetapkan opsi DHCP yang disetel ke VPC tempat direktori Anda berada. Dengan cara itu setiap instans dalam VPC dapat menunjuk ke domain tertentu, dan server DNS dapat menyelesaikan nama domain mereka.

Untuk informasi selengkapnya tentang set pilihan DHCP, lihat Buat set opsi DHCP.

Aktifkan Pengaturan Forwarder Bersyarat

Pengaturan penerusan bersyarat berikut Simpan forwarder bersyarat ini di Active Directory, replikasi sebagai berikut: harus diaktifkan. Mengaktifkan pengaturan ini akan mencegah pengaturan forwarder bersyarat menghilang ketika node diganti karena kegagalan infrastruktur atau kegagalan kelebihan beban.

Men-deploy pengendali domain tambahan

Secara default, AWS buat dua pengontrol domain yang ada di Availability Zone terpisah. Hal ini memberikan ketahanan kesalahan selama patch perangkat lunak dan peristiwa lain yang dapat membuat satu pengendali domain tidak terjangkau atau tidak tersedia. Kami merekomendasikan Anda men-deploy pengendali domain tambahan untuk lebih meningkatkan ketahanan dan memastikan performa menskalakan keluar dalam peristiwa dari peristiwa jangka panjang yang mempengaruhi akses ke pengendali domain atau Availability Zone.

Untuk informasi selengkapnya, lihat Menggunakan layanan locator Windows DC.

Memahami pembatasan nama pengguna untuk aplikasi AWS

AWS Directory Service memberikan dukungan untuk sebagian besar format karakter yang dapat digunakan dalam pembangunan nama pengguna. Namun, ada batasan karakter yang diberlakukan pada nama pengguna yang akan digunakan untuk masuk ke AWS aplikasi, seperti, Amazon, WorkSpaces WorkDocs Amazon WorkMail, atau Amazon. QuickSight Pembatasan ini mengharuskan karakter berikut tidak digunakan:

- Spasi
- Karakter multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Simbol @ diperbolehkan selama itu mendahului akhiran UPN.

Menggunakan direktori Anda

Berikut adalah beberapa saran yang perlu diingat saat menggunakan direktori Anda.

Jangan mengubah pengguna, grup, dan unit organisasi yang telah ditetapkan

Saat Anda menggunakan AWS Directory Service untuk meluncurkan direktori, AWS buat unit organisasi (OU) yang berisi semua objek direktori Anda. OU ini, yang memiliki nama NetBIOS yang Anda ketik saat membuat direktori Anda, terletak di root domain. Root domain dimiliki dan dikelola oleh AWS. Beberapa grup dan pengguna administratif juga dibuat.

Jangan memindahkan, menghapus atau dengan cara lain mengubah objek yang telah ditetapkan. Melakukannya dapat membuat direktori Anda tidak dapat diakses oleh Anda sendiri dan AWS. Untuk informasi selengkapnya, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.

Gabung domain secara otomatis

Saat meluncurkan instance Windows yang akan menjadi bagian dari AWS Directory Service domain, seringkali paling mudah untuk bergabung dengan domain sebagai bagian dari proses pembuatan instance daripada menambahkan instance secara manual nanti. Untuk menggabungkan domain secara otomatis, cukup pilih direktori yang benar untuk Direktori penggabungan domain saat meluncurkan instans baru. Anda dapat menemukan detailnya di Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory.

Atur kepercayaan dengan benar

Saat menyiapkan hubungan kepercayaan antara direktori Microsoft AD yang AWS Dikelola dan direktori lain, perhatikan panduan ini:

- Jenis kepercayaan harus cocok di kedua sisi (Forest atau Eksternal)
- Pastikan arah kepercayaan diatur dengan benar jika menggunakan kepercayaan satu arah (Keluar pada domain terpercaya, Masuk pada domain terpercaya)
- Nama domain yang memenuhi syarat (FQDNS) dan nama NetBIOS harus unik antara forest / domain

Untuk detail selengkapnya dan petunjuk spesifik tentang cara mengatur hubungan kepercayaan, lihat Menciptakan hubungan kepercayaan.

Mengelola direktori Anda

Pertimbangkan saran ini untuk mengelola direktori Anda.

Lacak kinerja pengontrol domain Anda

Untuk membantu mengoptimalkan keputusan penskalaan dan meningkatkan ketahanan dan kinerja direktori, sebaiknya gunakan metrik. CloudWatch Untuk informasi selengkapnya, lihat Pantau pengontrol domain Anda dengan metrik kinerja.

Untuk petunjuk tentang cara mengatur metrik pengontrol domain menggunakan CloudWatch konsol, lihat Cara mengotomatiskan penskalaan AWS Microsoft AD Terkelola berdasarkan metrik pemanfaatan di Blog Keamanan. AWS

Berhati-hati merancang ekstensi skema

Terapkan ekstensi skema dengan cermat untuk mengindeks direktori Anda untuk kueri yang penting dan sering. Berhati-hati untuk tidak over-indeks direktori karena indeks mengkonsumsi ruang direktori dan dengan cepat mengubah nilai-nilai yang diindeks dapat mengakibatkan masalah performa. Untuk menambahkan indeks, Anda harus membuat file Lightweight Directory Access Protocol (LDAP) Directory Interchange Format (LDIF) dan memperpanjang perubahan skema Anda. Untuk informasi selengkapnya, lihat Perpanjang skema Anda.

Tentang penyeimbang beban

Jangan gunakan penyeimbang beban di depan titik akhir Microsoft AD yang AWS Dikelola. Microsoft dirancang Direktori Aktif (AD) untuk digunakan dengan pengendali domain (DC) penemuan algoritme yang menemukan DC operasional paling responsif tanpa eksternal penyeimbangan beban. Penyeimbang beban jaringan eksternal secara tidak akurat mendeteksi DC aktif dan dapat mengakibatkan aplikasi Anda dikirim ke DC yang datang tetapi tidak siap untuk digunakan. Untuk informasi selengkapnya, lihat Load balancer dan Active Directory di Microsoft TechNet yang merekomendasikan untuk memperbaiki aplikasi agar menggunakan Active Directory dengan benar daripada menerapkan penyeimbang beban eksternal.

Buat backup instans Anda

Jika Anda memutuskan untuk menambahkan instance secara manual ke AWS Directory Service domain yang ada, buat cadangan atau ambil snapshot dari instance tersebut terlebih dahulu. Hal

ini sangat penting ketika menggabungkan instans Linux. Beberapa prosedur digunakan untuk menambahkan instans, jika tidak dilakukan dengan benar, dapat membuat instans Anda tidak terjangkau atau tidak dapat digunakan. Untuk informasi selengkapnya, lihat Snapshot atau pulihkan direktori Anda.

Mengatur olahpesan SNS

Dengan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) ketika status direktori Anda berubah. Anda akan diberi tahu jika direktori Anda berjalan dari status Aktif ke status Gangguan atau Tidak bisa dioperasi. Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Juga ingat bahwa jika Anda memiliki topik SNS yang menerima pesan dari AWS Directory Service, sebelum menghapus topik itu dari konsol Amazon SNS, Anda harus mengaitkan direktori Anda dengan topik SNS yang berbeda. Jika tidak, Anda berisiko kehilangan pesan status direktori penting. Untuk informasi tentang cara mengatur Amazon SNS, lihat Konfigurasikan pemberitahuan status direktori dengan Amazon SNS.

Terapkan pengaturan layanan direktori

AWS Microsoft AD yang dikelola memungkinkan Anda menyesuaikan konfigurasi keamanan untuk memenuhi persyaratan kepatuhan dan keamanan Anda. AWS Microsoft AD yang dikelola menyebarkan dan memelihara konfigurasi ke semua pengontrol domain di direktori Anda, termasuk saat menambahkan wilayah baru atau pengontrol domain tambahan. Anda dapat mengonfigurasi dan menerapkan pengaturan keamanan ini untuk semua direktori baru dan yang sudah ada. Anda dapat melakukan ini di konsol dengan mengikuti langkah-langkah di dalam Edit pengaturan keamanan direktori atau melalui UpdateSettings API.

Untuk informasi selengkapnya, lihat Konfigurasikan pengaturan keamanan direktori.

Hapus aplikasi Amazon Enterprise sebelum menghapus direktori

Sebelum menghapus direktori yang terkait dengan satu atau beberapa Aplikasi Amazon Enterprise seperti,, Amazon WorkSpaces Application Manager WorkSpaces, Amazon, Amazon WorkDocs WorkMail AWS Management Console, atau Amazon Relational Database Service (Amazon RDS), Anda harus terlebih dahulu menghapus setiap aplikasi. Untuk informasi selengkapnya untuk cara menghapus aplikasi ini, lihat Menghapus iklan Microsoft yang AWS Dikelola.

Menggunakan klien SMB 2.x saat mengakses saham SYSVOL dan NETLOGON

Komputer klien menggunakan Blok Pesan Server (SMB) untuk mengakses saham SYSVOL dan NETLOGON pada pengontrol domain AWS Microsoft AD Terkelola untuk Kebijakan Grup, skrip login, dan file lainnya. AWS Microsoft AD yang dikelola hanya mendukung SMB versi 2.0 (SMBv2) dan yang lebih baru.

SMBv2 dan protokol versi yang lebih baru menambahkan sejumlah fitur yang meningkatkan performa klien dan meningkatkan keamanan pengendali domain dan klien. Perubahan ini mengikuti rekomendasi oleh Tim Kesiapan Darurat Komputer Amerika Serikat dan Microsoft para menonaktifkan SMBv1.

> **Important**
>
> Jika Anda saat ini menggunakan klien SMBv1 untuk mengakses saham SYSVOL dan NETLOGON dari pengendali domain Anda, Anda harus memperbarui klien tersebut untuk menggunakan SMBv2 atau yang lebih baru. Direktori Anda akan berfungsi dengan benar tetapi klien SMBv1 Anda akan gagal terhubung ke saham SYSVOL dan NETLOGON dari pengontrol domain Microsoft AD AWS Terkelola Anda, dan juga tidak akan dapat memproses Kebijakan Grup.

Klien SMBv1 akan bekerja dengan server file SMBv1 kompatibel lainnya yang Anda miliki. Namun, AWS merekomendasikan agar Anda memperbarui semua server dan klien SMB Anda ke SMBv2 atau yang lebih baru. Untuk mempelajari selengkapnya tentang menonaktifkan SMBv1 dan memperbaruinya ke versi SMB yang lebih baru di sistem Anda, lihat postingan ini di Microsoft dan Support. TechNet

Melacak Koneksi Jarak Jauh SMBv1

Anda dapat meninjau log Peristiwa Windows Microsoft-Windows-SMBServer/Audit dari jarak jauh yang menghubungkan ke pengontrol domain AWS Microsoft AD Terkelola, setiap peristiwa dalam log ini menunjukkan koneksi SMBv1. Berikut adalah contoh informasi yang mungkin Anda lihat di salah satu log berikut:

Akses SMB1

Alamat Klien: ###.#####. ###

Bimbingan:

Peristiwa ini menunjukkan bahwa klien berusaha untuk mengakses server menggunakan SMB1. Untuk berhenti mengaudit akses SMB1, gunakan Windows PowerShell cmdlet Set-. SmbServerConfiguration

Memprogram aplikasi Anda

Sebelum memprogram aplikasi Anda, pertimbangkan hal berikut:

Menggunakan layanan locator Windows DC

Saat mengembangkan aplikasi, gunakan layanan pencari lokasi Windows DC atau gunakan layanan Dynamic DNS (DDNS) dari AWS Microsoft AD yang Dikelola untuk menemukan pengontrol domain (DC). Jangan hard code aplikasi dengan alamat DC. Layanan locator DC membantu memastikan beban direktori didistribusikan dan memungkinkan Anda untuk mengambil keuntungan dari penskalaan horizontal dengan menambahkan pengendali domain untuk deployment Anda. Jika Anda mengikat aplikasi ke DC tetap dan DC mengalami patch atau pemulihan, aplikasi Anda akan kehilangan akses ke DC bukannya menggunakan salah satu DC yang tersisa. Selain itu, hard coding DC dapat mengakibatkan hot spotting pada DC tunggal. Pada kasus yang parah, hot spotting dapat menyebabkan DC Anda menjadi tidak responsif. Kasus seperti itu juga dapat menyebabkan otomatisasi AWS direktori menandai direktori sebagai terganggu dan dapat memicu proses pemulihan yang menggantikan DC yang tidak responsif.

Muat tes sebelum diluncurkan ke produksi

Pastikan untuk melakukan pengujian laboratorium dengan aplikasi dan permintaan yang mewakili beban kerja produksi Anda untuk mengonfirmasi bahwa direktori menskalakan ke beban aplikasi Anda. Jika Anda memerlukan kapasitas tambahan, uji dengan DC tambahan saat mendistribusikan permintaan antara DC. Untuk informasi selengkapnya, lihat Men-deploy pengendali domain tambahan.

Gunakan kueri LDAP yang efisien

Kueri LDAP luas ke pengendali domain pada puluhan ribu objek dapat mengkonsumsi siklus CPU yang signifikan dalam DC tunggal, mengakibatkan hot spotting. Hal ini dapat mempengaruhi aplikasi yang berbagi DC yang sama selama kueri.

Kuota Microsoft AD yang Dikelola AWS

Berikut ini adalah kuota default untuk Microsoft AD yang Dikelola AWS. Kecuali dinyatakan lain, masing-masing kuota adalah per Region.

Kuota Microsoft AD yang Dikelola AWS

Resource	Kuota default
Direktori Microsoft AD yang Dikelola AWS	20
Snapshot manual *	5 per Microsoft AD yang Dikelola AWS
Umur snapshot manual **	180 hari
Jumlah maksimum pengendali domain per direktori	20
Domain bersama per Iklan Microsoft Standar***	5
Domain bersama untuk Perusahaan Microsoft AD***	125
Jumlah maksimum dari sertifikat otoritas sertifikasi (CA) terdaftar per direktori	5
Jumlah maksimum totalAWSDaerah dalam satuAWSDikelola Microsoft AD (Enterprise Edition) direktori****	5

* Kuota snapshot manual tidak dapat diubah.

** Usia maksimum yang didukung dari snapshot manual adalah 180 hari dan tidak dapat diubah. Hal ini disebabkan oleh atribut Masa Hidup-Tombstone dari objek dihapus yang menentukan umur simpan yang berguna dari backup keadaan sistem dari Direktori Aktif. Tidak mungkin memulihkan dari snapshot yang lebih tua dari 180 hari. Untuk informasi selengkapnya, lihat Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif di situs web Microsoft.

*** Kuota default domain bersama mengacu pada jumlah akun yang dapat dibagikan ke direktori individual.

**** Ini termasuk 1 Wilayah utama dan hingga 4 Wilayah tambahan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.

> **Note**
>
> Anda tidak dapat melampirkan alamat IP publik ke elastic network interface (ENI) AWS Anda.

Untuk informasi mengenai desain aplikasi dan distribusi beban, lihat Memprogram aplikasi Anda.

Untuk kuota penyimpanan dan objek, lihat Tabel Perbandinganpada halaman Penetapan harga Directory Service AWS.

Kompatibilitas aplikasi untuk Microsoft AD yang AWS Dikelola

AWS Directory Service untuk Microsoft Active Directory (AWS Managed Microsoft AD) kompatibel dengan beberapa AWS layanan dan aplikasi pihak ketiga.

Berikut ini adalah daftar AWS aplikasi dan layanan yang kompatibel:

- Amazon Chime - Untuk instruksi detail, lihat Menghubungkan ke Direktori Aktif Anda.
- Amazon Connect - Untuk informasi selengkapnya, lihat Cara kerja Amazon Connect.
- Amazon EC2 - Untuk informasi lebih lanjut, lihat. Bergabunglah dengan instans Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola
- Amazon QuickSight - Untuk informasi selengkapnya, lihat Mengelola akun pengguna di Amazon QuickSight Enterprise Edition.
- Amazon RDS for MySQL - Untuk informasi selengkapnya, lihat Menggunakan autentikasi Kerberos untuk MySQL.
- Amazon RDS for Oracle - Untuk informasi selengkapnya, lihat Menggunakan autentikasi Kerberos dengan Amazon RDS for Oracle.
- Amazon RDS for PostgreSQL - Untuk informasi selengkapnya, lihat Menggunakan autentikasi Kerberos dengan Amazon RDS for PostgreSQL.
- Amazon RDS for SQL Server - Untuk informasi selengkapnya, lihatMenggunakan autentikasi Windows dengan instans DB Amazon RDS Microsoft SQL Server.
- Amazon WorkDocs - Untuk petunjuk mendetail, lihat Menyambungkan ke direktori lokal Anda dengan Microsoft AD yang AWS Dikelola.
- Amazon WorkMail - Untuk petunjuk terperinci, lihat Mengintegrasikan Amazon WorkMail dengan direktori yang ada (penyiapan standar).

- AWS Client VPN - Untuk petunjuk terperinci, lihat Otentikasi dan otorisasi klien.
- AWS IAM Identity Center - Untuk petunjuk terperinci, lihat Connect IAM Identity Center ke Active Directory lokal.
- AWS License Manager - Untuk informasi selengkapnya, lihat Langganan berbasis pengguna di. AWS License Manager
- AWS Management Console — Untuk informasi lebih lanjut, lihatMengaktifkan akses ke AWS Management Console dengan kredensial AD.
- FSx for Windows File Server - Untuk informasi selengkapnya, lihat Apa itu FSx for Windows File Server? .
- WorkSpaces - Untuk petunjuk mendetail, lihat Meluncurkan WorkSpace menggunakan Microsoft AD yang AWS Dikelola.

Karena besarnya off-the-shelf aplikasi kustom dan komersial yang menggunakan Active Directory, AWS tidak dan tidak dapat melakukan verifikasi formal atau luas kompatibilitas aplikasi pihak ketiga dengan AWS Directory Service untuk Microsoft Active Directory (AWS Managed Microsoft AD). Meskipun AWS bekerja dengan pelanggan dalam upaya untuk mengatasi tantangan instalasi aplikasi potensial yang mungkin mereka hadapi, kami tidak dapat menjamin bahwa aplikasi apa pun atau akan terus kompatibel dengan Microsoft AD yang AWS Dikelola.

Aplikasi pihak ketiga berikut ini kompatibel dengan Microsoft AD yang AWS Dikelola:

- Aktivasi Berbasis Direktori Aktif (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra(sebelumnya dikenal sebagai Azure Active Directory (AzureAD))
- Microsoft Entra Connect(sebelumnya dikenal sebagai) Azure Active Directory Connect
- Distributed File System Replication (DFSR)
- Distributed File System Namespaces (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(termasuk SQL Server Selalu Pada Grup Ketersediaan)

- Microsoft System Center Configuration Manager(SCCM) - Pengguna yang menggunakan SCCM harus menjadi anggota grup Administrator Manajemen Sistem AWS Delegasi.
- Microsoft Windows and Windows Server OS
- Office 365

Perhatikan bahwa tidak semua konfigurasi dari aplikasi-aplikasi ini mungkin didukung.

Pedoman kompatibilitas

Meskipun aplikasi mungkin memiliki konfigurasi yang tidak kompatibel, konfigurasi deployment aplikasi sering dapat mengatasi ketidakcocokan. Berikut ini menjelaskan alasan paling umum untuk ketidakcocokan aplikasi. Pelanggan dapat menggunakan informasi ini untuk menyelidiki karakteristik kompatibilitas aplikasi yang diinginkan dan mengidentifikasi perubahan deployment yang potensial.

- Administrator domain atau izin istimewa lainnya – Beberapa aplikasi menyatakan bahwa Anda harus menginstalnya sebagai administrator domain. Karena AWS harus mempertahankan kontrol eksklusif tingkat izin ini untuk memberikan Active Directory sebagai layanan terkelola, Anda tidak dapat bertindak sebagai administrator domain untuk menginstal aplikasi tersebut. Namun, Anda sering dapat menginstal aplikasi tersebut dengan mendelegasikan izin khusus, kurang istimewa, dan AWS didukung kepada orang yang melakukan instalasi. Untuk detail selengkapnya tentang izin yang tepat yang diperlukan aplikasi Anda, tanyakan penyedia aplikasi Anda. Untuk informasi selengkapnya tentang izin yang AWS memungkinkan Anda mendelegasikan, lihat. Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola
- Akses ke Active Directory kontainer istimewa — Dalam direktori Anda, Microsoft AD AWS Terkelola menyediakan Unit Organisasi (OU) di mana Anda memiliki kontrol administratif penuh. Anda tidak memiliki izin membuat atau menulis dan mungkin memiliki izin baca terbatas untuk kontainer yang lebih tinggi di pohon Direktori Aktif daripada OU Anda. Aplikasi yang membuat atau mengakses kontainer yang tidak Anda miliki izinnya mungkin tidak bekerja. Namun, aplikasi semacam itu sering memiliki kemampuan untuk menggunakan kontainer yang Anda buat di OU Anda sebagai alternatif. Periksa dengan penyedia aplikasi Anda untuk menemukan cara untuk membuat dan menggunakan kontainer di OU Anda sebagai alternatif. Untuk informasi selengkapnya tentang mengelola OU Anda, lihat Cara mengelola Microsoft AD yang Dikelola AWS.
- Perubahan skema selama alur kerja penginstalan — Beberapa Active Directory aplikasi memerlukan perubahan pada skema Active Directory default, dan mereka mungkin mencoba menginstal perubahan tersebut sebagai bagian dari alur kerja instalasi aplikasi. Karena sifat istimewa ekstensi skema, AWS memungkinkan hal ini dengan mengimpor file Lightweight Directory

Interchange Format (LDIF) melalui konsol AWS Directory Service , CLI, atau SDK saja. Aplikasi semacam itu sering datang dengan file LDIF yang dapat Anda terapkan ke direktori melalui proses pembaruan AWS Directory Service skema. Untuk informasi selengkapnya tentang bagaimana proses impor LDIF bekerja, lihat Tutorial: Memperluas skema AD Microsoft yang AWS Dikelola. Anda dapat menginstal aplikasi dengan cara untuk memotong instalasi skema selama proses instalasi.

Aplikasi tidak kompatibel dikenal

Berikut daftar off-the-shelf aplikasi komersial yang biasa diminta yang belum kami temukan konfigurasi yang berfungsi dengan Microsoft AD yang AWS Dikelola. AWS memperbarui daftar ini dari waktu ke waktu atas kebijakannya sendiri sebagai sopan santun untuk membantu Anda menghindari upaya yang tidak produktif. AWS memberikan informasi ini tanpa jaminan atau klaim mengenai kompatibilitas saat ini atau masa depan.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

AWS Tutorial lab uji Microsoft AD yang dikelola

Bagian ini menyediakan serangkaian tutorial terpandu untuk membantu Anda membangun lingkungan lab pengujian AWS tempat Anda dapat bereksperimen dengan Microsoft AD yang AWS Dikelola.

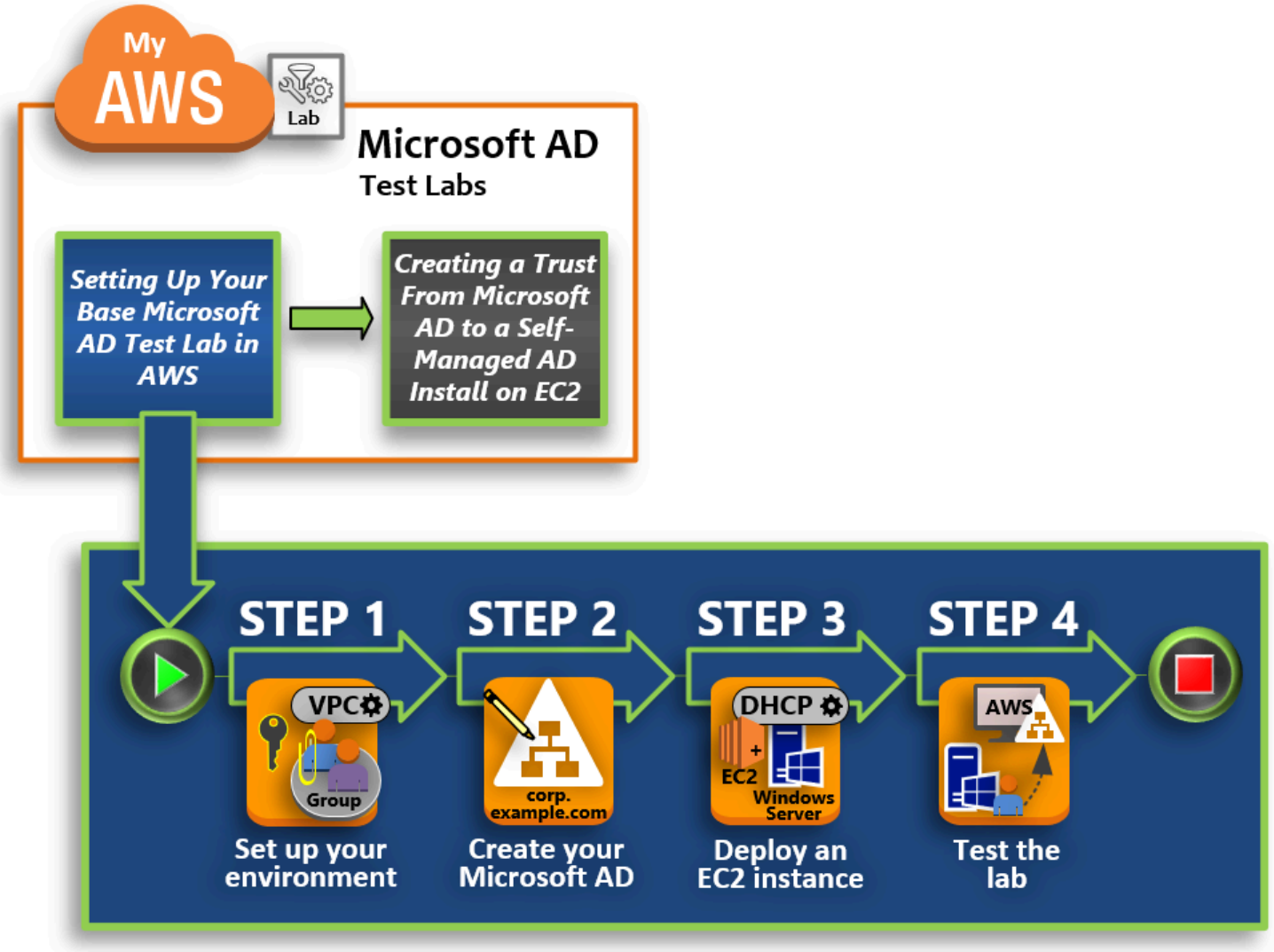
Topik

- Tutorial: Menyiapkan lab uji Microsoft AD AWS Terkelola basis Anda di AWS
- Tutorial: Membuat kepercayaan dari Microsoft AD yang Dikelola AWS ke instalasi Direktori Aktif yang dikelola sendiri pada Amazon EC2

Tutorial: Menyiapkan lab uji Microsoft AD AWS Terkelola basis Anda di AWS

Tutorial ini mengajarkan Anda cara mengatur AWS lingkungan Anda untuk mempersiapkan instalasi Microsoft AD AWS Terkelola baru yang menggunakan instans Amazon EC2 baru yang menjalankan Windows Server 2019. Ini kemudian mengajarkan Anda untuk menggunakan alat administrasi Direktori Aktif khas untuk mengelola lingkungan Microsoft AD yang AWS Dikelola dari instans EC2 Windows Anda. Pada saat Anda menyelesaikan tutorial, Anda akan mengatur prasyarat jaringan dan telah mengkonfigurasi hutan AD AWS Microsoft yang Dikelola baru.

Seperti yang ditunjukkan dalam ilustrasi berikut, lab yang Anda buat dari tutorial ini adalah komponen dasar untuk pembelajaran langsung tentang Managed AWS Microsoft AD. Anda dapat menambahkan tutorial opsional nanti untuk pengalaman langsung yang lebih banyak. Seri tutorial ini sangat ideal untuk siapa saja yang baru akan Microsoft AD yang Dikelola AWS dan menginginkan laboratorium pengujian untuk tujuan evaluasi. Tutorial ini memakan waktu sekitar 1 jam untuk menyelesaikannya.



[Langkah 1: Siapkan AWS lingkungan Anda untuk Direktori Aktif Microsoft AD yang AWS Dikelola]

Setelah menyelesaikan tugas prasyarat, Anda membuat dan mengonfigurasi VPC Amazon di instans EC2 Anda.

[Langkah 2: Buat Direktori Aktif Microsoft AD AWS Terkelola]

Pada langkah ini, Anda mengatur iklan Microsoft yang AWS Dikelola AWS untuk pertama kalinya.

[Langkah 3: Menerapkan instans Amazon EC2 untuk mengelola Direktori Aktif Microsoft AD yang AWS Dikelola]

Di sini, Anda menelusuri berbagai tugas pasca deployment yang diperlukan untuk komputer klien untuk terhubung ke domain baru Anda dan mengatur sistem Windows Server baru di EC2.

Langkah 4: Verifikasi bahwa laboratorium pengujian dasar beroperasi

Akhirnya, sebagai administrator, Anda memverifikasi bahwa Anda dapat masuk dan terhubung ke Microsoft AD yang Dikelola AWS dari sistem Windows Server di EC2. Setelah Anda berhasil menguji bahwa laboratorium beroperasi, Anda dapat terus menambahkan modul panduan laboratorium pengujian lainnya.

Prasyarat

Jika Anda berencana untuk menggunakan hanya langkah-langkah UI dalam tutorial ini untuk membuat laboratorium pengujian Anda, Anda dapat melewatkan bagian prasyarat ini dan melanjutkan ke Langkah 1. Namun, jika Anda berencana untuk menggunakan AWS CLI perintah atau AWS Tools for Windows PowerShell modul untuk membuat lingkungan lab pengujian Anda, Anda harus terlebih dahulu mengonfigurasi berikut ini:

- Pengguna IAM dengan akses dan kunci akses rahasia — Pengguna IAM dengan kunci akses diperlukan jika Anda ingin menggunakan AWS CLI atau AWS Tools for Windows PowerShell modul. Jika Anda tidak memiliki access key, lihat Membuat, memodifikasi, dan melihat access key (AWS Management Console).
- AWS Command Line Interface (opsional) - Unduh dan Instal AWS CLI pada Windows. Setelah diinstal, buka prompt perintah atau Windows PowerShell jendela, lalu ketik`aws configure`. Perhatikan bahwa Anda memerlukan access key dan kunci rahasia untuk menyelesaikan pengaturan. Lihat prasyarat pertama untuk langkah-langkah tentang cara melakukannya. Anda akan diminta hal berikut:
  - AWS ID kunci akses [Tidak ada]: `AKIAIOSFODNN7EXAMPLE`
  - AWS kunci akses rahasia [Tidak ada]: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - Nama Region default [Tidak ada]: `us-west-2`
  - Format keluar default [Tidak ada]: `json`
- AWS Tools for Windows PowerShell (opsional) – Unduh dan instal versi terbaru AWS Tools for Windows PowerShell dari https://aws.amazon.com/powershell/, dan kemudian jalankan perintah berikut. Perhatikan bahwa Anda memerlukan access key dan kunci rahasia Anda untuk menyelesaikan pengaturan. Lihat prasyarat pertama untuk langkah-langkah tentang cara melakukannya.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Langkah 1: Siapkan AWS lingkungan Anda untuk Direktori Aktif Microsoft AD yang AWS Dikelola

Sebelum dapat membuat Microsoft AD AWS Terkelola di lab AWS pengujian, Anda harus terlebih dahulu menyiapkan key pair Amazon EC2 agar semua data login dienkripsi.

Membuat key pair

Jika Anda sudah memiliki key pair, Anda dapat melewati langkah ini. Untuk informasi selengkapnya tentang pasangan kunci Amazon EC2, lihat Membuat pasangan kunci.

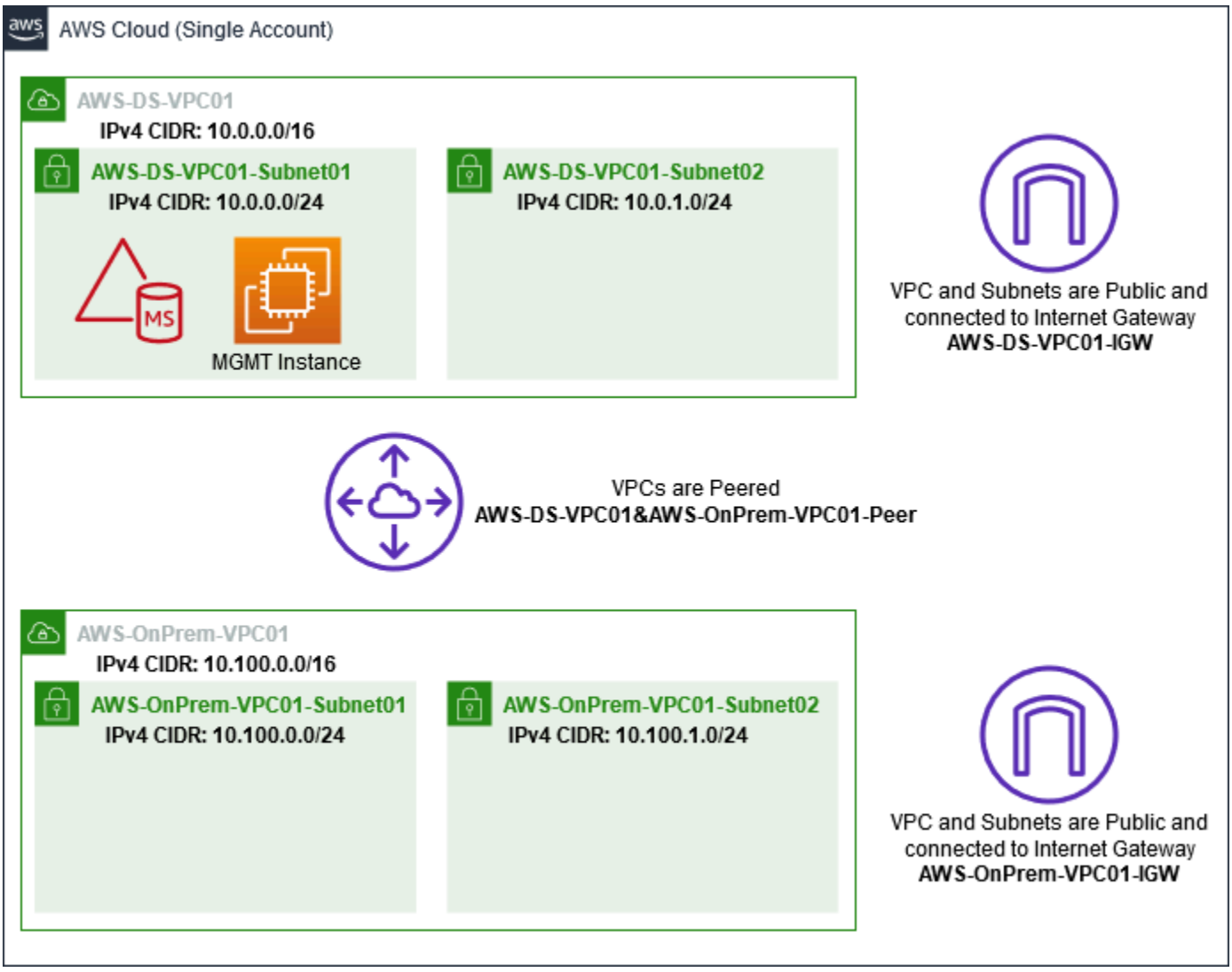
Untuk membuat pasangan kunci

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi, di bawah Jaringan & Keamanan, pilih Key Pair, dan kemudian pilih Buat Key Pair.
3. Untuk Nama key pair, ketik **`AWS-DS-KP`**. Untuk Format file key pair, pilih pem, lalu pilih Buat.
4. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Nama file adalah nama yang Anda tentukan ketika Anda membuat key pair Anda dengan ekstensi `.pem`. Simpan file kunci privat di suatu tempat yang aman.

> **Important**
>
> Ini adalah satu-satunya kesempatan bagi Anda untuk menyimpan file kunci pribadi. Anda harus menyediakan nama key pair Anda saat meluncurkan sebuah instans dan kunci pribadi yang terkait setiap kali Anda mendekripsi kata sandi untuk instans tersebut.

Buat, konfigurasikan, dan peer dua VPC Amazon

Seperti yang ditunjukkan dalam ilustrasi berikut, pada saat Anda menyelesaikan proses multi-langkah ini Anda akan membuat dan mengkonfigurasi dua VPC publik, dua subnet publik per VPC, satu Gateway Internet per VPC, dan satu Peering VPC koneksi antara VPC. Kami memilih untuk menggunakan VPC dan subnet publik untuk tujuan kesederhanaan dan biaya. Untuk beban kerja produksi, kami menyarankan Anda agar menggunakan VPC pribadi. Untuk informasi selengkapnya tentang meningkatkan keamanan VPC, lihat Keamanan dalam Amazon Virtual Private Cloud.



Semua AWS CLI dan PowerShell contoh menggunakan informasi VPC dari bawah dan dibangun di us-barat-2. Anda dapat memilih Region yang didukung mana pun untuk membangun lingkungan Anda. Untuk informasi umum, lihat Apa yang Dimaksud dengan Amazon VPC?.

Langkah 1: Buat dua VPC

Pada langkah ini, Anda perlu membuat dua VPC di akun yang sama menggunakan parameter yang ditentukan dalam tabel berikut. AWS Microsoft AD yang dikelola mendukung penggunaan akun terpisah dengan Bagikan direktori Anda fitur tersebut. VPC pertama akan digunakan untuk Managed AWS Microsoft AD. VPC kedua akan digunakan untuk sumber daya yang dapat digunakan nanti di Tutorial: Membuat kepercayaan dari Microsoft AD yang Dikelola AWS ke instalasi Direktori Aktif yang dikelola sendiri pada Amazon EC2.

Informasi VPC Direktori Aktif Terkelola	Informasi VPC lokal
Tag nama: AWS-DS-VPC01	Tag nama: AWS- OnPrem -VPC01
Blok CIDR IPv4: 10.0.0.0/16	Blok CIDR IPv4: 10.100.0.0/16
Blok CIDR IPv6: Tidak ada Blok CIDR IPv6	Blok CIDR IPv6: Tidak ada Blok CIDR IPv6
Penghunian: Default	Penghunian: Default

Untuk instruksi detail, lihat Membuat VPC.

Langkah 2: Buat dua subnet per VPC

Setelah Anda telah membuat VPC Anda perlu untuk membuat dua subnet per VPC menggunakan parameter yang ditentukan dalam tabel berikut. Untuk laboratorium pengujian ini setiap subnet akan menjadi /24. Ini akan memungkinkan hingga 256 alamat yang dikeluarkan per subnet. Setiap subnet harus dalam AZ terpisah. Menempatkan setiap subnet secara terpisah di AZ adalah salah satu AWS Prasyarat Microsoft AD yang dikelola.

Informasi subnet AWS-DS-VPC01:	AWS- OnPrem -VPC01 informasi subnet
Tag nama: AWS-ds-vpc01-subnet01	Tag nama: AWS- OnPrem -vpc01-subnet01
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx-DS-VPC 01 AWS	VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem
Availability Zone: us-west-2a	Availability Zone: us-west-2a
Blok CIDR IPv4: 10.0.0.0/24	Blok CIDR IPv4: 10.100.0.0/24
Tag nama: AWS-ds-vpc01-subnet02	Tag nama: AWS- OnPrem -vpc01-subnet02
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx-DS-VPC 01 AWS	VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem
Availability Zone: us-west-2b	Availability Zone: us-west-2b
Blok CIDR IPv4: 10.0.1.0/24	Blok CIDR IPv4: 10.100.1.0/24

Untuk instruksi detail, lihat Membuat subnet dalam VPC Anda.

Langkah 3: Buat dan lampirkan Internet Gateway ke VPC Anda

Karena kita menggunakan VPC publik Anda akan perlu untuk membuat dan melampirkan gateway Internet ke VPC Anda menggunakan parameter yang ditentukan dalam tabel berikut. Hal ini akan memungkinkan Anda untuk terhubung ke dan mengelola instans EC2 Anda.

Informasi Gateway Internet AWS-DS-VPC01	AWS- Informasi OnPrem Gateway Internet - VPC01
Tag nama: AWS-DS-VPC01-IGW	Tag nama: AWS- OnPrem -VPC01-IGW
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx-DS-VPC 01 AWS	VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem

Untuk instruksi detail, lihat Gateway internet.

Langkah 4: Konfigurasikan koneksi peering VPC antara AWS-DS-VPC01 dan - -VPC01 AWS OnPrem

Karena Anda sudah membuat dua VPC sebelumnya, Anda perlu menghubungkan mereka bersama-sama menggunakan peering VPC menggunakan parameter yang ditentukan dalam tabel berikut. Meskipun ada banyak cara untuk menghubungkan VPC Anda, tutorial ini akan menggunakan VPC Peering. AWS Microsoft AD yang dikelola mendukung banyak solusi untuk menghubungkan VPC Anda, beberapa di antaranya termasuk peering VPC, Transit Gateway, dan VPN.

Tag nama koneksi peering: AWS-DS-VPC01 & -AWS-VPC01-Peer OnPrem
VPC (Pemohon): vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS
Akun: Akun Saya
Region: Region Ini
VPC (Penerima): vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Untuk instruksi tentang cara membuat Koneksi Peering VPC dengan VPC lain dari dengan akun Anda, lihat Membuat koneksi peering VPC dengan VPC lain di akun Anda.

Langkah 5: Tambahkan dua rute ke setiap tabel rute utama VPC

Agar Gateway Internet dan Koneksi Peering VPC yang dibuat pada langkah sebelumnya fungsional, Anda perlu memperbarui tabel rute utama kedua VPC menggunakan parameter yang ditentukan pada tabel berikut. Anda akan menambahkan dua rute; 0.0.0.0/0 yang akan merutekan ke semua tujuan yang tidak diketahui secara eksplisit ke tabel rute dan 10.0.0.0/16 atau 10.100.0.0/16 yang akan merutekan ke setiap VPC melalui Koneksi Peering VPC yang dibangun di atas.

Anda dapat dengan mudah menemukan tabel rute yang benar untuk setiap VPC dengan memfilter pada tag nama VPC (-DS-VPC01 atau AWS- -VPC01). AWS OnPrem

Informasi rute 1 AWS-DS-VPC01	Informasi rute 2 AWS-DS-VPC01	AWS- OnPrem -VPC01 rute 1 Informasi	AWS- OnPrem -VPC01 rute 2 Informasi
Tujuan: 0.0.0.0/0 Target: igw-xxxxx xxxxxxxxxxxxx -DS-VPC01-IGW AWS	Tujuan: 10.100.0.0/16 Target: pcx-xxxxx xxxxxxxxxxxxxxx -DS-VPC01 & AWS- -vpc01-rekan AWS OnPrem	Tujuan: 0.0.0.0/0 Target: AWS igw-xxxxxxxxxxxxxxxxxx -onprem-vpc01	Tujuan: 10.0.0.0/16 Target: pcx-xxxxx xxxxxxxxxxxxxxx -DS-VPC01 & AWS- -vpc01-rekan AWS OnPrem

Untuk instruksi tentang cara menambahkan rute ke tabel rute VPC, lihat Menambahkan dan menghapus rute dari tabel rute.

Membuat grup keamanan untuk instans Amazon EC2

Secara default, Microsoft AD yang AWS Dikelola membuat grup keamanan untuk mengelola lalu lintas di antara pengontrol domainnya. Pada bagian ini, Anda perlu membuat 2 grup keamanan (satu untuk setiap VPC) yang akan digunakan untuk mengelola lalu lintas dalam VPC Anda untuk instans EC2 Anda menggunakan parameter yang ditentukan dalam tabel berikut. Anda juga menambahkan aturan yang mengizinkan RDP (3389) masuk dari mana saja dan untuk semua jenis lalu lintas masuk dari VPC lokal. Untuk informasi selengkapnya, lihat Grup keamanan Amazon EC2 untuk instans Windows.

Informasi grup keamanan AWS-DS-VPC01:
Nama grup keamanan: AWS DS Test Lab Security Group
Deskripsi: Grup Keamanan Lab Uji AWS DS
VPC: vpc-xxxxxxxxxxxxxxxxxxxxxxxxx-DS-VPC01 AWS

Aturan Masuk Grup Keamanan untuk AWS-DS-VPC01

Tipe	Protokol	Rentang port	Sumber	Jenis lalu lintas
Aturan TCP Kustom	TCP	3389	IP saya	Desktop Jarak Jauh
Semua Lalu Lintas	Semua	Semua	10.0.0.0/16	Semua lalu lintas VPC lokal

Aturan Keluar Grup Keamanan untuk AWS-DS-VPC01

Tipe	Protokol	Rentang Port	Tujuan	Jenis lalu lintas
Semua Lalu Lintas	Semua	Semua	0.0.0.0/0	Semua Lalu lintas

AWS- OnPrem -VPC01 informasi kelompok keamanan:
Nama grup keamanan: Grup Keamanan Lab AWS OnPrem Uji.
Deskripsi: Kelompok Keamanan Lab AWS OnPrem Uji.
VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem

Aturan Masuk Grup Keamanan untuk AWS- OnPrem -VPC01

Tipe	Protokol	Rentang port	Sumber	Jenis lalu lintas
Aturan TCP Kustom	TCP	3389	IP saya	Desktop Jarak Jauh
Aturan TCP Kustom	TCP	53	10.0.0.0/16	DNS
Aturan TCP Kustom	TCP	88	10.0.0.0/16	Kerberos
Aturan TCP Kustom	TCP	389	10.0.0.0/16	LDAP
Aturan TCP Kustom	TCP	464	10.0.0.0/16	Kerberos mengubah / mengatur kata sandi
Aturan TCP Kustom	TCP	445	10.0.0.0/16	SMB / CIFS
Aturan TCP Kustom	TCP	135	10.0.0.0/16	Replikasi
Aturan TCP Kustom	TCP	636	10.0.0.0/16	LDAP SSL
Aturan TCP Kustom	TCP	49152 - 65535	10.0.0.0/16	RPC
Aturan TCP Kustom	TCP	3268 - 3269	10.0.0.0/16	LDAP GC & LDAP GC SSL
Aturan UDP Kustom	UDP	53	10.0.0.0/16	DNS
Aturan UDP Kustom	UDP	88	10.0.0.0/16	Kerberos

Tipe	Protokol	Rentang port	Sumber	Jenis lalu lintas
Aturan UDP Kustom	UDP	123	10.0.0.0/16	Waktu Windows
Aturan UDP Kustom	UDP	389	10.0.0.0/16	LDAP
Aturan UDP Kustom	UDP	464	10.0.0.0/16	Kerberos mengubah / mengatur kata sandi
Semua Lalu Lintas	Semua	Semua	10.100.0.0/16	Semua lalu lintas VPC lokal

Aturan Keluar Grup Keamanan untuk AWS- OnPrem -VPC01

Tipe	Protokol	Rentang Port	Tujuan	Jenis lalu lintas
Semua Lalu Lintas	Semua	Semua	0.0.0.0/0	Semua Lalu lintas

Untuk intruksi detail tentang cara membuat dan menambahkan aturan ke grup keamanan Anda, lihat Cara menggunakan grup keamanan.

Langkah 2: Buat Direktori Aktif Microsoft AD AWS Terkelola

Anda dapat menggunakan tiga metode yang berbeda untuk membuat direktori Anda. Anda dapat menggunakan AWS Management Console prosedur (direkomendasikan untuk tutorial ini) atau Anda dapat menggunakan AWS Tools for Windows PowerShell prosedur AWS CLI atau untuk membuat direktori Anda.

Metode 1: Untuk membuat direktori Microsoft AD yang AWS Dikelola (AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih Microsoft AD yang Dikelola AWS , lalu pilih Selanjutnya.

3. Pada halaman Masukkan informasi direktori, berikan informasi berikut, dan pilih Selanjutnya.

   - Untuk Edisi, pilih salah satu antara Standard Edition atau Enterprise Edition. Untuk informasi selengkapnya tentang edisi, lihat Directory Service AWS untuk Microsoft Active Directory.
   - Untuk Nama DNS direktori, ketik **`corp.example.com`**.
   - Untuk Nama NetBIOS direktori, ketik **`corp`**.
   - Untuk Deskripsi direktori, ketik **`AWS DS Managed`**.
   - Untuk Kata sandi admin, ketik kata sandi yang ingin Anda gunakan untuk akun ini dan ketik lagi kata sandi di Konfirmasi kata sandi. Akun Admin ini secara otomatis dibuat selama proses pembuatan direktori. Kata sandi tidak dapat menyertakan kata admin. Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:
     - Huruf kecil (a-z)
     - Huruf besar (A-Z)
     - Angka (0-9)
     - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

   - Untuk VPC, pilih opsi yang dimulai dengan AWS-DS-VPC01 dan diakhiri dengan (10.0.0.0/16).
   - Untuk Subnet, pilih subnet publik 10.0.0.0/24 dan 10.0.1.0/24.
5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Membuat direktori membutuhkan waktu 20 sampai 40 menit. Setelah dibuat, nilai Status berubah ke Aktif.

Metode 2: Untuk membuat Microsoft AD yang AWS Dikelola (Windows PowerShell) (Opsional)

1. Buka Windows PowerShell.
2. Ketik perintah berikut ini. Pastikan untuk menggunakan nilai yang disediakan pada Langkah 4 dari prosedur sebelumnya. AWS Management Console

```
New-DSMicrosoftAD -Name corp.example.com –ShortName corp –Password P@ssw0rd
 –Description “AWS DS Managed” - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

Metode 3: Untuk membuat Microsoft AD yang AWS Dikelola (AWS CLI) (Opsional)

1. Buka AWS CLI.
2. Ketik perintah berikut ini. Pastikan untuk menggunakan nilai yang disediakan pada Langkah 4 dari prosedur sebelumnya. AWS Management Console

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

Langkah 3: Menerapkan instans Amazon EC2 untuk mengelola Direktori Aktif Microsoft AD yang AWS Dikelola

Untuk lab ini, kami menggunakan instans Amazon EC2 yang memiliki alamat IP publik agar mudah mengakses instans manajemen dari mana saja. Dalam pengaturan produksi, Anda dapat menggunakan instance yang ada di VPC pribadi yang hanya dapat diakses melalui VPN AWS Direct Connect atau tautan. Tidak ada persyaratan instans memiliki alamat IP publik.

Di bagian ini, Anda menelusuri berbagai tugas pasca deployment yang diperlukan untuk komputer klien untuk terhubung ke domain Anda menggunakan Windows Server baru di instans EC2 baru Anda. Anda menggunakan Windows Server pada langkah berikutnya untuk memverifikasi bahwa laboratorium beroperasi.

Opsional: Buat opsi DHCP diatur dalam AWS-DS-VPC01 untuk direktori Anda

Dalam prosedur opsional ini, Anda menyiapkan cakupan opsi DHCP sehingga instans EC2 di VPC Anda secara otomatis menggunakan AD AWS Microsoft Terkelola untuk resolusi DNS. Untuk informasi selengkapnya, lihat Set pilihan DHCP.

Untuk membuat set opsi DHCP untuk direktori Anda

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Set Opsi DHCP, lalu pilih Buat set opsi DHCP.
3. Pada halaman Buat set opsi DHCP, berikan nilai berikut untuk direktori Anda:
   - Untuk Nama, ketik **`AWS DS DHCP`**.
   - Untuk Nama domain, ketik **`corp.example.com`**.
   - Untuk Server nama domain, ketik alamat IP dari server DNS direktori yang disediakan AWS .

> **Note**
>
> Untuk menemukan alamat ini, buka halaman AWS Directory Service Direktori, lalu pilih ID direktori yang berlaku. Pada halaman Detail, identifikasi dan gunakan IP yang ditampilkan di alamat DNS.
> Atau, untuk menemukan alamat ini, buka halaman AWS Directory Service Direktori, dan pilih ID direktori yang berlaku. Kemudian, pilih Skala & bagikan. Di bawah pengontrol Domain, identifikasi dan gunakan IP yang ditampilkan di alamat IP.

- Biarkan pengaturan kosong untuk Server NTP, Server nama NetBIOS, dan Jenis simpul NetBIOS.

4. Pilih Buat set opsi DHCP, lalu pilih Tutup. Set pilihan DHCP yang baru muncul dalam daftar pilihan DHCP Anda.
5. Catat ID dari set pilihan DHCP yang baru (dopt-***xxxxxxxx***). Anda menggunakannya pada akhir prosedur ini ketika Anda mengasosiasikan set pilihan yang baru dengan VPC Anda.

> **Note**
>
> Penggabungan domain yang mulus bekerja tanpa harus mengkonfigurasi Set Pilihan DHCP.

6. Pada panel navigasi, pilih VPC Anda.
7. Dalam daftar VPC, pilih VPC DS AWS , Pilih Tindakan, lalu pilih Edit set pilihan DHCP.
8. Pada halaman Edit set pilihan DHCP, pilih set pilihan yang Anda catat di Langkah 5, dan kemudian pilih Simpan.

Membuat peran untuk menggabungkan instans Windows ke domain Microsoft AD AWS Terkelola

Gunakan prosedur ini untuk mengonfigurasi peran yang menggabungkan instans Amazon EC2 Windows ke domain. Untuk informasi selengkapnya, lihat Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory.

Untuk mengkonfigurasi EC2 untuk menggabungkan instans Windows ke domain Anda

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran, dan lalu pilih Buat peran.

3. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
4. Segera di bawah Pilih layanan yang akan menggunakan peran ini, pilih EC2, lalu pilih Berikutnya: Izin.
5. Di halaman Kebijakan izin terlampir, lakukan hal berikut:

   - Pilih kotak di samping kebijakan terkelola AmazonSSM ManagedInstanceCore. Kebijakan ini menyediakan izin minimum yang diperlukan untuk menggunakan layanan Systems Manager.
   - Pilih kotak di samping kebijakan terkelola AmazonSSM DirectoryServiceAccess. Kebijakan ini menyediakan izin untuk menggabungkan instans ke Direktori Aktif yang dikelola oleh AWS Directory Service.

   Untuk informasi tentang kebijakan terkelola ini dan kebijakan lain yang dapat dilampirkan ke profil instans IAM untuk Systems Manager, lihat Buat profil instans IAM untuk Systems Manager dalam Panduan Pengguna AWS Systems Manager . Untuk informasi selengkapnya tentang kebijakan terkelola , lihat Kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.
6. Pilih Berikutnya: Tag.
7. (Opsional) Tambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk peran ini, lalu pilih Selanjutnya: Tinjau.
8. Untuk nama Peran, masukkan nama untuk peran yang menjelaskan bahwa itu digunakan untuk menggabungkan instance ke domain, seperti DomainJoinEC2.
9. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
10. Pilih Buat peran. Sistem mengembalikan Anda ke halaman Peran.

Buat instans Amazon EC2 dan secara otomatis bergabung dengan direktori

Dalam prosedur ini Anda mengatur sistem Windows Server dalam instans EC2 yang dapat digunakan nanti untuk mengelola pengguna, grup, dan kebijakan di Active Directory.

Untuk membuat instans EC2 dan menggabungkan direktori secara otomatis

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pilih Luncurkan Instans.
3. Pada halaman Langkah 1, di sebelah Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxx*** pilih Pilih.

4. Pada halaman Langkah 2, pilih t3.micro (ingat, Anda dapat memilih jenis instans yang lebih besar), kemudian pilih Selanjutnya: Konfigurasi Detail Instans.
5. Pada halaman Langkah 3, lakukan hal berikut:
   - Untuk Jaringan, pilih VPC yang diakhiri dengan AWS-DS-VPC01 (misalnya, vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01).
   - Untuk Subnet pilih Subnet publik 1, yang harus dikonfigurasikan sebelumnya untuk Availability Zone pilihan Anda (misalnya, subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***us-west-2a***).
   - Untuk Tetapkan Otomatis IP Publik, pilih Aktifkan (jika pengaturan subnet tidak diatur untuk mengaktifkan secara default).
   - Untuk Direktori penggabungan domain, pilih corp.example.com (d-***xxxxxxxxxx***).
   - Untuk peran IAM pilih nama yang Anda berikan peran instans AndaMembuat peran untuk menggabungkan instans Windows ke domain Microsoft AD AWS Terkelola, seperti DomainJoinEC2.
   - Biarkan pengaturan lainnya pada default.
   - Pilih Berikutnya: Tambahkan Penyimpanan.
6. Pada halaman Langkah 4, biarkan pengaturan default, kemudian pilih Berikutnya: Tambahkan Tanda.
7. Pada halaman Langkah 5, pilih Tambahkan Tanda. Di bawah Kunci ketik **`corp.example.com-mgmt`** kemudian pilih Berikutnya: Konfigurasi Grup Keamanan.
8. Pada halaman Langkah 6, pilih Pilih grup keamanan yang ada, pilih AWS DS Test Lab Security Group (yang sebelumnya Anda atur dalam tutorial Dasar), lalu pilih Tinjau dan Luncurkan untuk meninjau instance Anda.
9. Pada halaman Langkah 7, tinjau halaman, dan kemudian pilih Luncurkan.
10. Pada kotak dialog Pilih key pair yang sudah ada atau buat key pair baru, lakukan hal berikut:
    - Pilih Pilih key pair yang sudah ada.
    - Di bawah Pilih key pair, pilih AWS-DS-KP.
    - Pilih kotak centang Saya mengakui….
    - Pilih Luncurkan Instans.
11. Pilih Lihat Instans untuk kembali ke konsol Amazon EC2 dan melihat status deployment.

Menginstal alat Direktori Aktif pada instans EC2 Anda

Anda dapat memilih dari dua metode untuk menginstal Active Directory Domain Management Tools pada instans EC2 Anda. Anda dapat menggunakan UI Server Manager (direkomendasikan untuk tutorial ini) atauWindows PowerShell.

Untuk menginstal alat Direktori Aktif pada instans EC2 Anda (Pengelola Server)

1. Di konsol Amazon EC2, pilih Instans, pilih Instans yang baru saja Anda buat, kemudian pilih Hubungkan.
2. Di kotak dialog Hubungkan ke Instans Anda, pilih Dapatkan Kata sandi untuk mengambil kata sandi jika Anda belum melakukannya, kemudian pilih Unduh File Remote Desktop.
3. Di kotak dialog Keamanan Windows, ketik kredensial administrator lokal Anda untuk Windows Server komputer untuk masuk (misalnya, **`administrator`**).
4. Dari menu Mulai, pilih Pengelola Server.
5. Di Dasbor, pilih Tambah Peran dan Fitur.
6. Di Tambahkan Wizard Peran dan Fitur, pilih Selanjutnya.
7. Pada halaman Pilih jenis instalasi, pilih Instalasi berbasis peran atau berbasis fitur, lalu pilih Selanjutnya.
8. Pada halaman Pilih server tujuan, pastikan bahwa server lokal dipilih, dan kemudian pilih Selanjutnya.
9. Pada halaman Pilih peran server, pilih Selanjutnya.
10. Pada halaman Pilih fitur, lakukan hal berikut:
    - Pilih kotak centang Pengelolaan Kebijakan Grup.
    - Perluas Alat Administrasi Server Jarak Jauh, dan kemudian perluas Alat Administrasi Peran.
    - Pilih kotak centang Alat AD DS dan AD LDS.
    - Pilih kotak centang Alat Server DNS.
    - Pilih Berikutnya.
11. Pada halaman Konfirmasi pilihan instalasi, tinjau informasi, lalu pilih Instal. Setelah penginstalan fitur selesai, alat baru berikut atau snap-in akan tersedia di folder Alat Administratif Windows di menu Mulai.
    - Pusat Administrasi Direktori Aktif
    - Domain dan Kepercayaan Direktori Aktif.

- Modul Direktori Aktif untuk Windows PowerShell
- Situs dan Layanan Direktori Aktif.
- Pengguna dan Komputer Direktori Aktif
- Edit ADSI
- DNS
- Pengelolaan Kebijakan Grup

Untuk menginstal alat Active Directory pada instans EC2 Anda (Windows PowerShell) (Opsional)

1. Mulai Windows PowerShell.
2. Ketik perintah berikut ini.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
Tools,RSAT-DNS-Server
```

Langkah 4: Verifikasi bahwa laboratorium pengujian dasar beroperasi

Gunakan prosedur berikut untuk memverifikasi bahwa laboratorium pengujian telah diatur dengan sukses sebelum menambahkan modul panduan laboratorium pengujian tambahan. Prosedur ini memverifikasi bahwa Windows Server Anda dikonfigurasi dengan tepat, dapat terhubung ke domain corp.example.com, dan digunakan untuk mengelola hutan AD Microsoft Terkelola Anda. AWS

Untuk memverifikasi bahwa laboratorium pengujian dasar beroperasi

1. Keluar dari instans EC2 di mana Anda masuk sebagai administrator lokal.
2. Kembali ke konsol Amazon EC2, pilih Instans pada panel navigasi. Kemudian pilih instans yang Anda buat. Pilih Hubungkan.
3. Di kotak dialog Hubungkan ke Instans Anda, pilih Unduh File Remote Desktop.
4. Di kotak dialog Keamanan Windows, ketik kredensial administrator Anda untuk domain CORP untuk masuk (misalnya, **`corp\admin`**).
5. Setelah Anda masuk, di menu Mulai, di bawah Alat Administratif Windows, pilih Pengguna dan Komputer Direktori Aktif.
6. Anda akan melihat corp.example.com ditampilkan dengan semua OU default dan akun yang terasosiasikan dengan domain baru. Di bawah Pengontrol Domain, perhatikan nama pengontrol

domain yang dibuat secara otomatis saat Anda membuat AD AWS Microsoft Terkelola kembali di Langkah 2 tutorial ini.

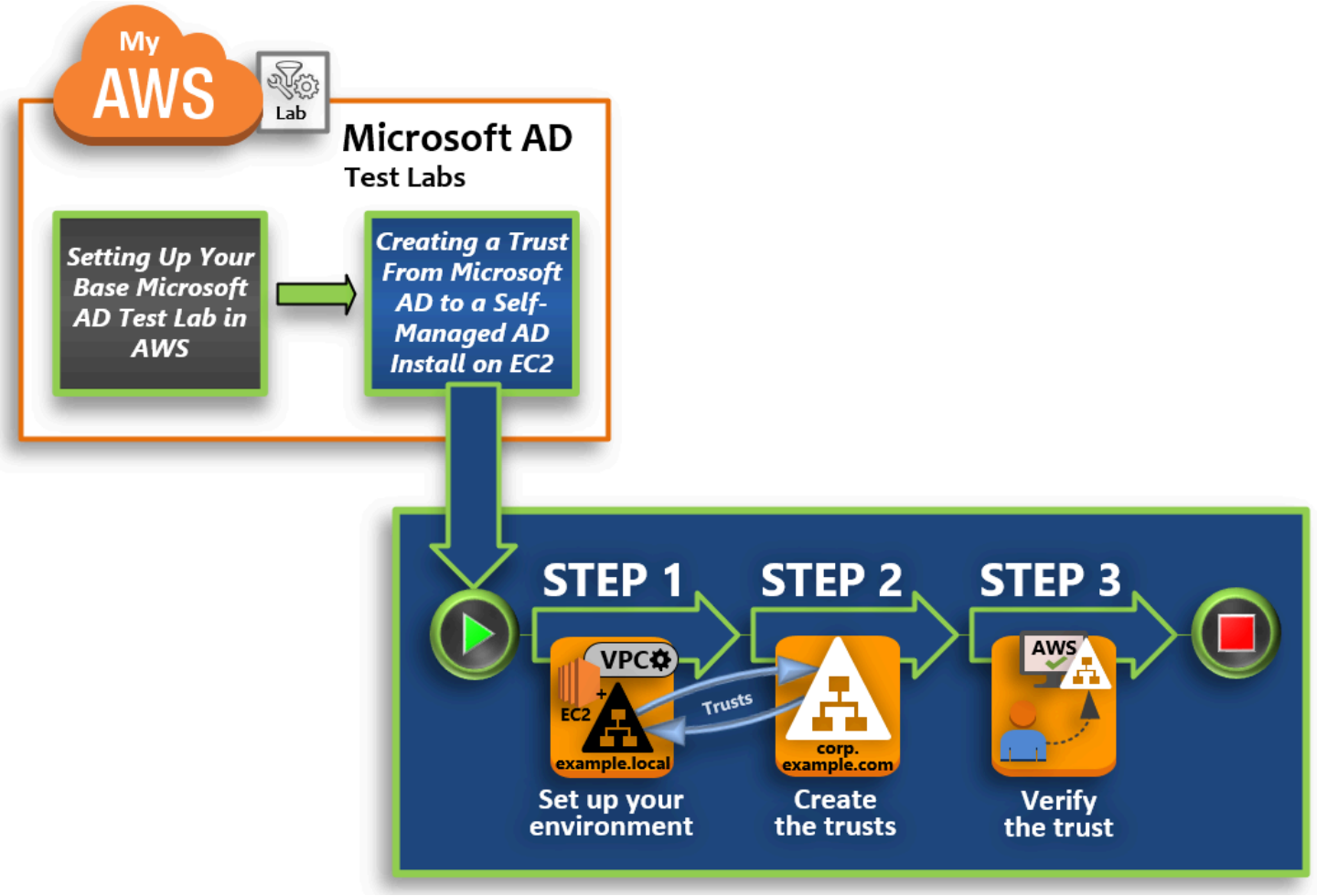
Selamat! Lingkungan lab pengujian dasar Microsoft AD AWS Terkelola Anda kini telah dikonfigurasi. Anda siap untuk mulai menambahkan laboratorium pengujian berikutnya dalam seri.

Tutorial berikutnya: Tutorial: Membuat kepercayaan dari Microsoft AD yang Dikelola AWS ke instalasi Direktori Aktif yang dikelola sendiri pada Amazon EC2

Tutorial: Membuat kepercayaan dari Microsoft AD yang Dikelola AWS ke instalasi Direktori Aktif yang dikelola sendiri pada Amazon EC2

Dalam tutorial ini, Anda akan mempelajari cara membuat kepercayaan antara Directory Service AWS untuk Microsoft Active Directory yang Anda buat di Tutorial dasar. Anda juga belajar untuk membuat forest Direktori Aktif asli yang baru pada Windows Server di Amazon EC2. Seperti ditunjukkan pada ilustrasi berikut, laboratorium yang Anda buat dari tutorial ini adalah blok bangunan kedua yang diperlukan saat menyiapkan laboratorium pengujian Microsoft AD yang Dikelola AWS yang lengkap. Anda dapat menggunakan laboratorium pengujian untuk menguji solusi AWS cloud murni atau berbasis cloud hybrid.

Anda hanya perlu membuat tutorial ini sekali. Setelah itu Anda dapat menambahkan tutorial opsional bila diperlukan untuk pengalaman lebih.



Langkah 1: Atur lingkungan Anda untuk kepercayaan

Sebelum Anda dapat membuat kepercayaan antara forest Direktori Aktif baru dan forest Microsoft AD yang Dikelola AWS yang Anda buat di Tutorial dasar, Anda perlu mempersiapkan lingkungan Amazon EC2 Anda. Untuk melakukannya, pertama Anda membuat server Windows Server 2019, promosikan server tersebut ke pengendali domain, dan kemudian konfigurasi VPC Anda sesuai dengannya.

Langkah 2: Buat trust

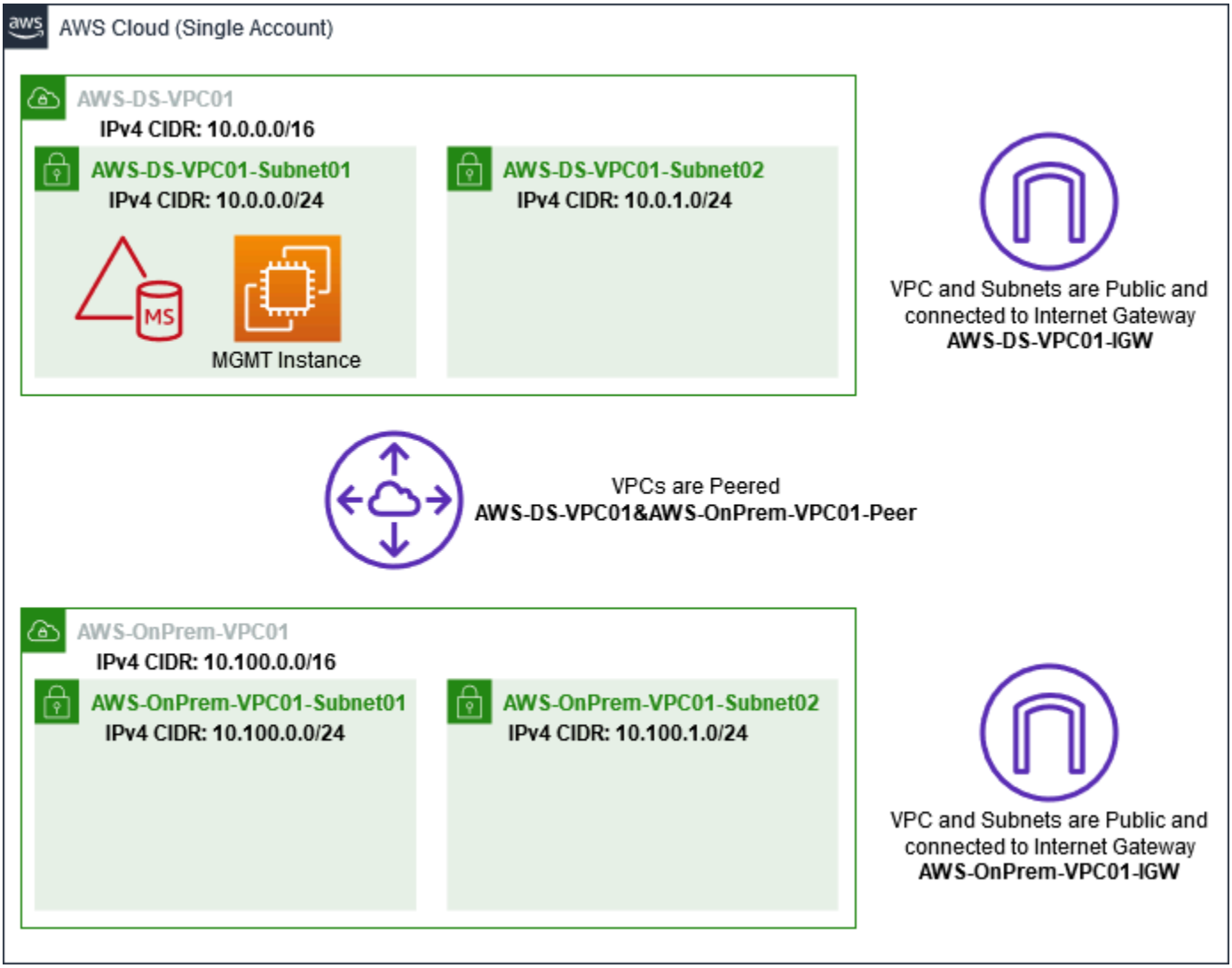
Pada langkah ini, Anda membuat hubungan kepercayaan forest dua arah antara forest Direktori Aktif baru yang di-host di Amazon EC2 dan forest Microsoft AD yang Dikelola AWS Anda di AWS.

Langkah 3: Verifikasi kepercayaan

Akhirnya, sebagai administrator, Anda menggunakan konsol AWS Directory Service tersebut untuk memverifikasi bahwa Trust baru beroperasi.

Langkah 1: Atur lingkungan Anda untuk kepercayaan

Pada bagian ini, Anda mengatur lingkungan Amazon EC2 Anda, men-deploy forest baru Anda, dan mempersiapkan VPC Anda untuk kepercayaan dengan AWS.



Membuat instans EC2 Windows Server 2019

Gunakan prosedur berikut untuk membuat server anggota Windows Server 2019 di Amazon EC2.

Untuk membuat instans EC2 Windows Server 2019

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di konsol Amazon EC2, pilih Luncurkan Instans.
3. Pada halaman Langkah 1, temukan Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxx*** di dalam daftar. Lalu pilih Pilih.

4. Pada halaman Langkah 2, pilih t2.large, lalu pilih Berikutnya: Konfigurasi Detail Instans.
5. Pada halaman Langkah 3, lakukan hal berikut:
   - Untuk Jaringan, pilih vpc- ***xxxxxxxxxxxxxxxxxx*** AWS - OnPrem -VPC01 (yang sebelumnya Anda atur di tutorial Base).
   - Untuk Subnet, pilih subnet - ***xxxxxxxxxxxxxxxxx*** | - -vpc01-subnet01 | - -VPC01. AWS OnPrem AWS OnPrem
   - Untuk daftar Tetapkan Otomatis IP Publik, pilih Aktifkan (jika pengaturan subnet tidak diatur ke Aktifkan secara default).
   - Biarkan pengaturan lainnya pada default.
   - Pilih Selanjutnya: Tambahkan Penyimpanan.
6. Pada halaman Langkah 4, biarkan pengaturan default, kemudian pilih Berikutnya: Tambahkan Tanda.
7. Pada halaman Langkah 5, pilih Tambahkan Tanda. Di bawah Kunci ketik **`example.local-DC01`**, kemudian pilih Berikutnya: Konfigurasi Grup Keamanan.
8. Pada halaman Langkah 6, pilih Pilih grup keamanan yang ada, pilih AWSOn-Prem Test Lab Security Group (yang sebelumnya Anda atur dalam tutorial Dasar), lalu pilih Tinjau dan Luncurkan untuk meninjau instance Anda.
9. Pada halaman Langkah 7, tinjau halaman, dan kemudian pilih Luncurkan.
10. Pada kotak dialog Pilih key pair yang sudah ada atau buat key pair baru, lakukan hal berikut:
    - Pilih Pilih key pair yang sudah ada.
    - Di bawah Pilih key pair, pilih AWS-DS-KP (yang sebelumnya Anda atur di Tutorial dasar).
    - Pilih kotak centang Saya mengakui….
    - Pilih Luncurkan Instans.
11. Pilih Lihat Instans untuk kembali ke konsol Amazon EC2 dan melihat status deployment.

Promosikan server Anda ke pengendali domain

Sebelum Anda dapat membuat kepercayaan, Anda harus membangun dan men-deploy pengendali domain pertama untuk forest baru. Selama proses ini Anda mengkonfigurasi forest Direktori Aktif baru, menginstal DNS, dan mengatur server ini untuk menggunakan server DNS lokal untuk resolusi nama. Anda harus me-reboot server pada akhir prosedur ini.

> **Note**
>
> Jika Anda ingin membuat pengendali domain di AWS yang bereplikasi dengan jaringan on-premise, Anda harus terlebih dahulu menggabungkan instans EC2 secara manual ke domain on-premise Anda. Setelah itu Anda dapat mempromosikan server ke pengendali domain.

Untuk mempromosikan server Anda ke pengendali domain

1. Di konsol Amazon EC2, pilih Instans, pilih Instans yang baru saja Anda buat, kemudian pilih Hubungkan.
2. Di kotak dialog Hubungkan ke Instans Anda, pilih Unduh File Remote Desktop.
3. Di kotak dialog Keamanan Windows, ketik kredensial administrator lokal Anda untuk komputer Windows Server untuk masuk (misalnya, **`administrator`**). Jika Anda belum memiliki kata sandi administrator lokal, kembali ke konsol Amazon EC2, klik kanan pada instans, dan pilih Dapatkan Kata Sandi Windows. Arahkan ke file `AWS DS KP.pem` Anda atau kunci `.pem` pribadi Anda, dan kemudian pilih Dekripsi Kata sandi.
4. Dari menu Mulai, pilih Pengelola Server.
5. Di Dasbor, pilih Tambah Peran dan Fitur.
6. Di Tambahkan Wizard Peran dan Fitur, pilih Selanjutnya.
7. Pada halaman Pilih jenis instalasi, pilih Instalasi berbasis peran atau berbasis fitur, lalu pilih Selanjutnya.
8. Pada halaman Pilih server tujuan, pastikan bahwa server lokal dipilih, dan kemudian pilih Selanjutnya.
9. Pada halaman Pilih peran server, pilih Layanan Domain Direktori Aktif. Di kotak dialog Tambahkan Wizard Peran dan Fitur, verifikasi bahwa kotak centang Sertakan alat manajemen (jika ada) dipilih. Pilih Tambahkan Fitur, lalu pilih Selanjutnya.
10. Pada halaman Pilih fitur, pilih Selanjutnya.
11. Pada halaman Layanan Domain Direktori Aktif, pilih Selanjutnya.
12. Pada halaman Konfirmasi pilihan instalasi, pilih Instal.
13. Setelah binari Direktori Aktif diinstal, pilih Tutup.
14. Ketika Pengelola Server terbuka, cari bendera di atas sebelah kata Kelola. Ketika bendera ini berubah kuning, server siap untuk dipromosikan.
15. Pilih bendera kuning, dan kemudian pilih Mempromosikan server ini ke pengendali domain.

16. Pada halaman Konfigurasi Deployment, pilih Menambahkan forest baru. Di Nama domain root ketik **`example.local`**, lalu pilih Selanjutnya.
17. Pada halaman Opsi Pengendali Domain, lakukan hal berikut:
    - Di Tingkat fungsional forest dan Tingkat fungsional domain, pilih Windows Server 2016.
    - Di bawah Tentukan kemampuan pengendali domain, verifikasikan bahwa Server Domain Name System (DNS) dan Katalog Global (GC) dipilih.
    - Ketik dan kemudian konfirmasikan kata sandi Directory Services Restore Mode (DSRM). Kemudian pilih Selanjutnya.
18. Pada halaman Opsi DNS, abaikan peringatan tentang delegasi dan pilih Selanjutnya.
19. Pada halaman Opsi tambahan, pastikan EXAMPLE terdaftar sebagai nama NetBios domain.
20. Pada halaman Jalur, biarkan default, dan kemudian pilih Selanjutnya.
21. Pada halaman Tinjau opsi, pilih Selanjutnya. Server sekarang memeriksa untuk memastikan semua prasyarat untuk pengendali domain terpenuhi. Anda mungkin melihat beberapa peringatan ditampilkan, namun Anda dapat mengabaikannya dengan aman.
22. Pilih Instal. Setelah instalasi selesai, server akan reboot dan kemudian menjadi pengendali domain fungsional.

Mengkonfigurasi VPC Anda

Tiga prosedur berikut memandu Anda melalui langkah-langkah untuk mengkonfigurasi VPC Anda untuk konektivitas dengan AWS.

Untuk mengkonfigurasi aturan keluar VPC Anda

1. Di AWS Directory Servicekonsol, catat ID direktori Microsoft AD AWS Terkelola untuk corp.example.com yang sebelumnya Anda buat di tutorial Base.
2. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
3. Di panel navigasi, pilih Grup Keamanan.
4. Cari ID direktori Microsoft AD yang Dikelola AWS Anda. Di hasil pencarian, pilih item dengan deskripsi AWS membuat grup keamanan untuk pengendali direktori d-***xxxxxx***.

> **Note**
>
> Grup keamanan ini secara otomatis dibuat ketika Anda awalnya membuat direktori Anda.

5. Pilih tab Aturan Keluar di bawah grup keamanan tersebut. Pilih Edit, pilih Tambahkan aturan lain, dan kemudian tambahkan nilai-nilai berikut:

   - Untuk Jenis, pilih Semua lalu lintas.
   - Untuk Tujuan, ketik **`0.0.0.0/0`**.
   - Biarkan pengaturan lainnya pada default.
   - Pilih Simpan.

Untuk memverifikasi praautentikasi kerberos diaktifkan

1. Pada pengendali domain example.local, buka Pengelola Server.
2. Pada menu Alat, pilih Pengguna dan komputer Direktori Aktif.
3. Arahkan ke direktori Pengguna, klik kanan pada pengguna mana pun dan pilih Properti, dan kemudian pilih tab Akun. Di daftar Opsi akun, gulir ke bawah dan pastikan bahwa Tidak memerlukan praautentikasi Kerberos tidak dicentang.
4. Lakukan langkah yang sama untuk domain corp.example.comdari instans corp.example.com-mgmt.

Untuk mengkonfigurasi DNS penerus bersyarat

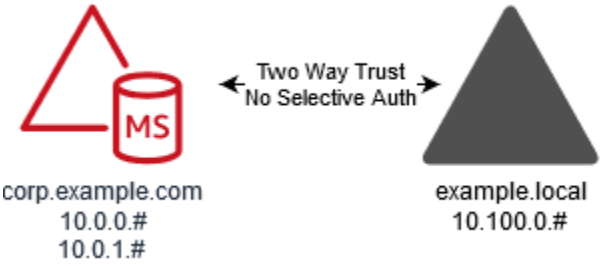
> **Note**
>
> Penerus bersyarat adalah server DNS pada jaringan yang digunakan untuk meneruskan kueri DNS sesuai dengan nama domain DNS dalam kueri tersebut. Sebagai contoh, server DNS dapat dikonfigurasi untuk meneruskan semua kueri yang diterima untuk nama yang berakhir dengan widgets.example.com ke alamat IP server DNS tertentu atau ke alamat IP dari beberapa server DNS.

1. Buka konsol AWS Directory Service.
2. Di panel navigasi, pilih Direktori.
3. Pilih ID direktori Microsoft AD yang Dikelola AWS Anda.
4. Perhatikan nama domain yang memenuhi syarat (FQDN), corp.example.com, dan alamat DNS dari direktori Anda.
5. Sekarang, kembali ke pengendali domain example.local, dan kemudian buka Pengelola Server.

6. Pada menu Alat, pilih DNS.
7. Pada pohon konsol, perluas server DNS dari domain di mana Anda mengatur kepercayaan, dan arahkan ke Penerus Bersyarat.
8. Klik kanan Penerus Bersyarat, lalu pilih Penerus Bersyarat Baru.
9. Dalam domain DNS, ketik **`corp.example.com`**.
10. Di bawah Alamat IP dari server utama, pilih <Klik di sini untuk menambahkan... >, ketik alamat DNS pertama dari direktori Microsoft AD yang Dikelola AWS Anda (yang Anda catat dalam prosedur sebelumnya), dan kemudian tekan Masukkan. Lakukan hal yang sama untuk alamat DNS kedua. Setelah memasukkan alamat DNS, Anda mungkin mendapatkan kesalahan “timeout” atau “tidak dapat menyelesaikan”. Anda biasanya dapat mengabaikan error ini.
11. Pilih kotak centang Menyimpan penerus bersyarat ini di Direktori Aktif dan mereplikasi sebagai berikut. Di menu drop-down, pilih Semua server DNS di Forest ini, lalu pilih OK.

Langkah 2: Buat trust

Di bagian ini, Anda membuat dua kepercayaan forest yang terpisah. Satu kepercayaan dibuat dari domain Direktori Aktif pada instans EC2 Anda dan yang lain dari Microsoft AD yang Dikelola AWS Anda di AWS.



Untuk membuat kepercayaan dari domain EC2 Anda ke Microsoft AD yang Dikelola AWS Anda

1. Masuk ke example.local.
2. Buka Pengelola Server dan di pohon konsol pilih DNS. Perhatikan alamat IPv4 yang tercantum untuk server. Anda akan membutuhkan ini dalam prosedur berikutnya ketika Anda membuat penerus bersyarat dari corp.example.com ke direktori example.local.
3. Pada menu Alat, pilih Domain Direktori Aktif dan Kepercayaan.
4. Pada pohon konsol tersebut, klik kanan example.local lalu pilih Properti.
5. Pada tab Kepercayaan, pilih Kepercayaan Baru, lalu pilih Selanjutnya.
6. Pada halaman Nama Kepercayaan, ketik **`corp.example.com`**, lalu pilih Selanjutnya.

7. Pada halaman Jenis kepercayaan, pilih Kepercayaan forest, lalu pilih Selanjutnya.

> **Note**
>
> Microsoft AD yang Dikelola AWS juga mendukung kepercayaan eksternal. Namun, untuk tujuan tutorial ini, Anda akan membuat kepercayaan forest dua arah.

8. Pada halaman Arah kepercayaan, pilih Dua arah, lalu pilih Selanjutnya.

> **Note**
>
> Jika nanti Anda memutuskan untuk mencoba ini dengan kepercayaan satu arah, pastikan arah kepercayaan diatur dengan benar (Keluar pada domain terpercaya, Masuk pada domain terpercaya). Untuk informasi umum, lihat Memahami arah kepercayaan pada situs web Microsoft.

9. Pada halaman Sisi Kepercayaan, pilih Hanya domain ini, lalu pilih Selanjutnya.
10. Pada halaman Autentikasi Kepercayaan Keluar, pilih Autentikasi seluruh forest, lalu pilih Selanjutnya.

> **Note**
>
> Meskipun Autentikasi selektif dalam pilihan, untuk kesederhanaan dari tutorial ini kami sarankan Anda tidak mengaktifkannya di sini. Saat dikonfigurasi itu membatasi akses melalui kepercayaan eksternal atau forest hanya untuk pengguna di domain terpercaya atau forest yang telah secara eksplisit diberikan izin autentikasi ke objek komputer (komputer sumber daya) yang berada di domain atau forest terpercaya. Untuk informasi selengkapnya, lihat Mengkonfigurasi pengaturan autentikasi selektif.

11. Pada halaman Kata sandi Kepercayaan, ketik kata sandi kepercayaan dua kali, dan kemudian pilih Selanjutnya. Anda akan menggunakan kata sandi yang sama ini pada prosedur berikutnya.
12. Pada halaman Pilihan Kepercayaan Selesai, tinjau hasilnya, dan kemudian pilih Selanjutnya.
13. Pada halaman Pembuatan Kepercayaan Selesai, tinjau hasilnya, dan kemudian pilih Selanjutnya.
14. Pada halaman Konfirmasi Kepercayaan Keluar, pilih Tidak, jangan konfirmasikan kepercayaan keluar. Lalu pilih Selanjutnya

15. Pada halaman Konfirmasi Kepercayaan Masuk, pilih Tidak, jangan konfirmasikan kepercayaan masuk. Lalu pilih Selanjutnya
16. Pada halaman Menyelesaikan Wizard Kepercayaan Baru, pilih Selesai.

> **Note**
>
> Hubungan kepercayaan adalah fitur global dari Microsoft AD yang Dikelola AWS. Jika Anda menggunakan Replikasi multi-Region, prosedur berikut harus dilakukan di Region primer. Perubahan akan diterapkan di semua Region yang direplikasi secara otomatis. Untuk informasi selengkapnya, lihat Fitur Global vs Regional.

Untuk membuat kepercayaan dari Microsoft AD yang Dikelola AWS Anda ke domain EC2 Anda.

1. Buka konsol AWS Directory Service.
2. Pilih direktori corp.example.com.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih Tindakan, dan kemudian pilih Tambahkan hubungan kepercayaan.
5. Di kotak dialog Tambahkan hubungan kepercayaan, lakukan hal berikut:
   - Di bawah Jenis kepercayaan pilih Kepercayaan forest.

     > **Note**
     >
     > Pastikan bahwa Jenis kepercayaan yang Anda pilih di sini cocok dengan jenis kepercayaan yang sama yang dikonfigurasi dalam prosedur sebelumnya (Untuk membuat kepercayaan dari domain EC2 Anda untuk Microsoft AD yang Dikelola AWS Anda).

   - Untuk Nama domain jarak jauh yang ada atau baru, ketik example.local.

- Untuk Kata sandi kepercayaan, ketik kata sandi yang sama yang Anda berikan dalam prosedur sebelumnya.
- Di bawah Arah kepercayaan, pilih Dua Arah.

> **Note**
>
> - Jika nanti Anda memutuskan untuk mencoba ini dengan kepercayaan satu arah, pastikan arah kepercayaan diatur dengan benar (Keluar pada domain terpercaya, Masuk pada domain terpercaya). Untuk informasi umum, lihat Memahami arah kepercayaan pada situs web Microsoft.
> - Meskipun Autentikasi selektif dalam pilihan, untuk kesederhanaan dari tutorial ini kami sarankan Anda tidak mengaktifkannya di sini. Saat dikonfigurasi itu membatasi akses melalui kepercayaan eksternal atau forest hanya untuk pengguna di domain terpercaya atau forest yang telah secara eksplisit diberikan izin autentikasi ke objek komputer (komputer sumber daya) yang berada di domain atau forest terpercaya. Untuk informasi selengkapnya, lihat Mengkonfigurasi pengaturan autentikasi selektif.

- Untuk Penerus bersyarat, ketik alamat IP server DNS Anda di forest example.local (yang Anda catat dalam prosedur sebelumnya).

> **Note**
>
> Penerus bersyarat adalah server DNS pada jaringan yang digunakan untuk meneruskan kueri DNS sesuai dengan nama domain DNS dalam kueri tersebut. Sebagai contoh, server DNS dapat dikonfigurasi untuk meneruskan semua kueri yang diterima untuk nama yang berakhir dengan widgets.example.com ke alamat IP server DNS tertentu atau ke alamat IP dari beberapa server DNS.

6. Pilih Tambahkan.

Langkah 3: Verifikasi kepercayaan

Di bagian ini, Anda menguji apakah kepercayaan berhasil diatur antara AWS dan Direktori Aktif di Amazon EC2.

Untuk memverifikasi kepercayaan

1. Buka konsol AWS Directory Service.
2. Pilih direktori corp.example.com.
3. Pada halaman Detail direktori, lakukan salah satu hal berikut:
   - Jika Anda memiliki beberapa Region yang ditampilkan di bawah Replikasi multi-Region, pilih Region primer, dan kemudian pilih tab Jaringan & keamanan. Untuk informasi selengkapnya, lihat Region utama vs tambahan.
   - Jika Anda tidak memiliki Region apa pun yang ditampilkan di bawah Replikasi Multi-Region, pilih tab Jaringan & keamanan.
4. Di bagian Hubungan kepercayaan, pilih hubungan kepercayaan yang baru saja Anda buat.
5. Pilih Tindakan, lalu pilih Verifikasi hubungan kepercayaan.

Setelah verifikasi selesai, Anda akan melihat Diverifikasiditampilkan di bawah kolom Status.

Selamat telah menyelesaikan tutorial ini! Anda sekarang memiliki lingkungan multiforest Direktori Aktif berfungsi penuh dari mana Anda dapat mulai menguji berbagai skenario. Tutorial laboratorium pengujian tambahan direncanakan pada tahun 2018, jadi periksa kembali sesekali untuk melihat apa yang baru.

Pemecahan Masalah AWS Microsoft AD yang Dikelola

Berikut ini dapat membantu Anda memecahkan beberapa masalah umum yang mungkin Anda alami saat membuat atau menggunakan direktori Anda.

Masalah dengan Microsoft AD yang AWS Dikelola

Beberapa tugas pemecahan masalah hanya dapat diselesaikan oleh. AWS Support Berikut adalah beberapa tugasnya:

- Mulai ulang pengontrol domain AWS Directory Service yang disediakan.
- Tingkatkan Direktori Aktif Microsoft AD AWS Terkelola.

Untuk membuat kasus dukungan, lihat Membuat kasus dukungan dan manajemen kasus.

Masalah dengan Netlogon dan komunikasi saluran aman

Sebagai mitigasi terhadap CVE-2020-1472, Microsoft telah merilis patch yang mengubah cara komunikasi saluran aman Netlogon diproses oleh pengendali domain. Sejak diperkenalkannya perubahan Netlogon aman ini, beberapa koneksi Netlogon (server, workstation, dan validasi kepercayaan) mungkin tidak diterima oleh Microsoft AD Anda yang Dikelola. AWS

Untuk memverifikasi apakah masalah Anda terkait dengan Netlogon atau komunikasi saluran aman, cari ID peristiwa 5827 di CloudWatch Log Amazon Anda (untuk masalah terkait otentikasi perangkat) atau 5828 (untuk masalah terkait validasi kepercayaan AD). Untuk selengkapnya tentang CloudWatch di Microsoft AD yang AWS Dikelola, lihatMengaktifkan penerusan log.

Untuk informasi selengkapnya tentang mitigasi terhadap CVE-2020-1472, lihat Cara mengelola perubahan dalam koneksi saluran aman Netlogon yang terkait dengan CVE-2020-1472 pada situs web Microsoft.

Pemulihan kata sandi

Jika pengguna lupa kata sandi atau mengalami masalah saat masuk ke direktori Simple AD atau Microsoft AD yang AWS Dikelola, Anda dapat mengatur ulang kata sandi mereka menggunakan direktori AWS Management Console, Windows PowerShell atau direktori. AWS CLI

Untuk informasi selengkapnya, lihat Mengatur ulang kata sandi pengguna.

Sumber daya tambahan

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengannya. AWS

- AWS Pusat Pengetahuan —Temukan FAQ dan tautan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- AWS Support Center —Dapatkan dukungan teknis.
- AWS Pusat Support Premium —Dapatkan dukungan teknis premium.

Topik

- Memantau DNS Server dengan Microsoft Event Viewer
- Kesalahan menggabungkan domain Linux

- Direktori aktif ruang penyimpanan yang tersedia rendah
- Kesalahan ekstensi skema
- Alasan status pembuatan kepercayaan

Memantau DNS Server dengan Microsoft Event Viewer

Anda dapat audit peristiwa DNS Microsoft AD yang Dikelola AWS, sehingga lebih mudah untuk mengidentifikasi dan memecahkan masalah DNS. Misalnya, jika catatan DNS hilang, Anda dapat menggunakan log peristiwa audit DNS untuk membantu mengidentifikasi akar masalah dan memperbaiki masalah. Anda juga dapat menggunakan log peristiwa audit DNS untuk meningkatkan keamanan dengan mendeteksi dan memblokir permintaan dari alamat IP yang mencurigakan.

Untuk melakukan itu, Anda harus masuk dengan akun Admin atau dengan akun yang merupakan anggota dari grup Administrator Sistem Nama Domain AWS. Untuk informasi selengkapnya tentang grup ini, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.

Untuk mengakses Event Viewer untuk Microsoft AD DNS AWS Terkelola

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Pada panel navigasi kiri, pilih Instans.
3. Temukan instans Amazon EC2 yang digabungkan ke direktori Microsoft AD yang Dikelola AWS Anda. Pilih instans, lalu pilih Hubungkan.
4. Setelah terhubung ke instans Amazon EC2, buka menu Start dan pilih folder Windows Administrative Tools. Dalam folder Alat Administratif, pilih Penampil Acara.
5. Di jendela Penampil peristiwa, pilih Tindakan lalu pilih Hubungkan ke Komputer Lain.
6. Pilih Komputer lain, ketik salah satu nama server DNS Microsoft AD yang Dikelola AWS atau alamat IP, dan pilih OK.
7. Di panel sebelah kiri, arahkan ke Log Aplikasi dan Layanan>Microsoft>Windows>DNS-Server, dan kemudian pilih Audit.

Kesalahan menggabungkan domain Linux

Berikut ini dapat membantu Anda memecahkan masalah beberapa pesan kesalahan yang mungkin Anda alami ketika menggabungkan instans EC2 Linux ke direktori Microsoft AD yang Dikelola AWS.

Instans Linux tidak dapat menggabungkan domain atau mengautentikasi

Instans Ubuntu 14.04, 16.04, dan 18.04 harus reverse-resolvable di DNS sebelum ranah dapat bekerja dengan Microsoft Active Directory. Jika tidak, Anda mungkin akan menjumpai salah satu dari dua skenario berikut:

Skenario 1: Instans Ubuntu yang belum bergabung ke ranah

Untuk instans Ubuntu yang mencoba bergabung dengan ranah, perintah `sudo realm join` mungkin tidak memberikan izin yang diperlukan untuk menggabungkan domain dan mungkin menampilkan kesalahan berikut:

! Tidak dapat mengautentikasi ke direktori aktif: SASL (-1): kegagalan generik: GSSAPI Kesalahan: Nama yang tidak valid diberikan (Sukses) adcli: tidak dapat terhubung ke EXAMPLE.COM domain: Tidak dapat mengautentikasi ke direktori aktif: SASL (-1): kegagalan generik: GSSAPI Kesalahan: Nama yang tidak valid diberikan (Sukses)! Izin tidak mencukupi untuk bergabung dengan ranah domain: Tidak dapat bergabung dengan ranah: Izin tidak mencukupi untuk bergabung dengan domain

Skenario 2: Instans Ubuntu yang bergabung ke ranah

Untuk instance Ubuntu yang sudah bergabung dengan domain Microsoft Active Directory, upaya SSH ke instance menggunakan kredenal domain mungkin gagal dengan kesalahan berikut:

$ ssh admin@EXAMPLE.COM @198 .51.100

tidak ada identitas seperti itu: /Users/username/.ssh/id_ed25519: Tidak ada file atau direktori seperti itu

Kata sandi admin@EXAMPLE.COM @198 .51.100:

Izin ditolak, silakan coba lagi.

Kata sandi admin@EXAMPLE.COM @198 .51.100:

Jika Anda masuk ke instans dengan kunci publik dan mencentang `/var/log/auth.log`, Anda mungkin melihat kesalahan berikut tentang tidak dapat menemukan pengguna:

12 Mei 01:02:12 ip-192-0-2-0 sshd [2251]: pam_unix (sshd: auth): kegagalan otentikasi; nama log = uid = 0 euid = 0 tty = ssh ruser = rhost = 203.0.113.0

12 Mei 01:02:12 ip-192-0-2-0 sshd [2251]: pam_sss (sshd: auth): kegagalan otentikasi; nama log = uid = 0 euid = 0 tty = ssh ruser= rhost = 203.0.113.0 pengguna = admin@EXAMPLE.COM

12 Mei 01:02:12 ip-192-0-2-0 sshd [2251]: pam_sss (sshd:auth): diterima untuk pengguna admin@EXAMPLE.COM: 10 (Pengguna tidak diketahui modul otentikasi yang mendasarinya)

12 Mei 01:02:14 ip-192-0-2-0 sshd [2251]: Kata sandi gagal untuk pengguna yang tidak valid admin@EXAMPLE.COM dari 203.0.113.0 port 13344 ssh2

12 Mei 01:02:15 ip-192-0-2-0 sshd [2251]: Koneksi ditutup oleh 203.0.113.0 [preauth]

Namun, `kinit` untuk pengguna masih bekerja. Lihat contoh ini:

ubuntu @ip -192-0-2-0: ~$ kinit admin@EXAMPLE.COM Kata sandi untuk admin@EXAMPLE.COM: ubuntu @ip -192-0-2-0: ~$ klist Cache tiket: FILE: /tmp/krb5cc_1000 Prinsip default: admin@EXAMPLE.COM

Solusi

Solusi yang direkomendasikan saat ini untuk kedua skenario ini adalah untuk menonaktifkan DNS terbalik di `/etc/krb5.conf` di bagian [libdefaults] seperti yang ditunjukkan di bawah ini:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Masalah autentikasi kepercayaan satu arah dengan penggabungan domain secara mulus.

Jika Anda memiliki kepercayaan keluar satu arah yang dibuat antara iklan Microsoft AWS Terkelola dan Direktori Aktif lokal, Anda mungkin mengalami masalah autentikasi saat mencoba mengautentikasi terhadap instance Linux yang bergabung dengan domain menggunakan kredensi Direktori Aktif tepercaya Anda dengan Winbind.

Kesalahan

31 Juli 00:00:00 EC2amaz-LSMWQT sshd [23832]: Kata sandi gagal untuk user@corp.example.com dari xxx.xxx.xxx.xxx port 18309 ssh2

31 Jul 00:05:00 EC2amaz-LSMWqt sshd [23832]: pam_winbind (sshd: auth): mendapatkan kata sandi (0x00000390)

31 Jul 00:05:00 EC2amaz-LSMWqt sshd [23832]: pam_winbind (sshd:auth): pam_get_item mengembalikan kata sandi

31 Jul 00:05:00 EC2AMAZ-LSMWQT sshd [23832]: pam_winbind (sshd:auth): permintaan wbcLogonUser gagal: WBC_ERR_AUTH_ERROR, kesalahan PAM: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, Pesan kesalahan adalah: Nama objek tidak ditemukan.

31 Juli 00:05:00 EC2amaz-LSMWqt sshd [23832]: pam_winbind (sshd:auth): kesalahan modul internal (retval = PAM_SYSTEM_ERR (4), pengguna = 'CORP\ user')

Solusi

Untuk mengatasi masalah ini, Anda perlu untuk mengomentari atau menghapus direktif dari file konfigurasi modul PAM (`/etc/security/pam_winbind.conf`) menggunakan langkah-langkah berikut.

1. Buka file `/etc/security/pam_winbind.conf` di editor teks.

   ```
   sudo vim /etc/security/pam_winbind.conf
   ```

2. Mengomentari atau menghapus direktif berikut krb5_auth = yes.

   ```
   [global]

   cached_login = yes
   krb5_ccache_type = FILE
   #krb5_auth = yes
   ```

3. Menghentikan layanan Winbind, dan kemudian mulai lagi.

   ```
   service winbind stop or systemctl stop winbind
   net cache flush
   service winbind start or systemctl start winbind
   ```

Direktori aktif ruang penyimpanan yang tersedia rendah

Saat Microsoft AD yang Dikelola AWS terganggu karena Direktori Aktif memiliki ruang penyimpanan yang tersedia rendah, tindakan segera diperlukan untuk mengembalikan direktori ke keadaan aktif. Dua penyebab paling umum dari gangguan ini dibahas pada bagian di bawah ini:

1. Folder SYSVOL menyimpan lebih dari objek kebijakan grup yang esensial
2. Basis data Direktori Aktif telah mengisi volume

Untuk informasi harga tentang penyimpanan Microsoft AD yang Dikelola AWS, lihat Harga AWS Directory Service.

Folder SYSVOL menyimpan lebih dari objek kebijakan grup yang esensial

Penyebab umum dari gangguan ini adalah karena untuk menyimpan file yang non-esensial untuk pemrosesan kebijakan grup di folder SYSVOL. File non-esensial ini bisa menjadi EXE, MSI, atau file lain yang non esensial untuk diproses Kebijakan Grup. Objek esensial untuk diproses Kebijakan Grup adalah objek Kebijakan Grup, Skrip masuk/keluar, dan Central Store untuk objek Kebijakan Grup. Setiap file non-esensial harus disimpan di server file selain pengendali domain Microsoft AD yang Dikelola AWS Anda.

Jika file untuk Instalasi Perangkat Lunak Kebijakan Grup diperlukan Anda harus menggunakan server file untuk menyimpan file-file instalasi tersebut. Jika Anda lebih memilih untuk tidak mengelola sendiri server file, AWS menyediakan opsi server file terkelola, Amazon FSx.

Untuk menghapus file yang tidak diperlukan Anda dapat mengakses share SYSVOL melalui jalur universal penamaan konvensi (UNC). Misalnya, jika nama domain yang memenuhi syarat (FQDN) Anda adalah example.com, jalur UNC untuk SYSVOL adalah “\\example.local\SYSVOL\example.local\”. Setelah Anda menemukan dan menghapus objek yang non-esensial bagi kebijakan grup untuk memproses direktori, itu akan kembali ke keadaan Aktif dalam waktu 30 menit. Jika setelah 30 menit direktori tidak aktif, silahkan hubungi AWS Support.

Menyimpan file Kebijakan Grup penting saja di bagian SYSVOL Anda akan memastikan bahwa Anda tidak akan mengganggu direktori Anda karena SYSVOL penuh.

Basis data Direktori Aktif telah mengisi volume

Penyebab umum dari gangguan ini adalah karena basis data Direktori Aktif memenuhi volume. Untuk memverifikasi apakah ini masalahnya, Anda dapat meninjau jumlah total objek dalam direktori anda. Kami menebalkan kata total untuk memastikan bahwa Anda memahami objek yang dihapus masih dihitung dalam jumlah total objek dalam sebuah direktori.

Secara default Microsoft AD yang Dikelola AWS menyimpan item dalam Keranjang Sampah AD selama 180 hari sebelum mereka menjadi Objek-Daur ulang. Setelah objek menjadi Objek-Daur ulang (tombstoned), objek itu dipertahankan selama 180 hari sebelum akhirnya dibersihkan dari

direktori. Jadi ketika sebuah objek dihapus itu ada di dalam basis data direktori untuk 360 hari sebelum dibersihkan. Inilah sebabnya mengapa jumlah total objek perlu dievaluasi.

Untuk detail selengkapnya tentang jumlah total objek yang didukung Microsoft AD yang Dikelola AWS, lihat Harga AWS Directory Service.

Untuk mendapatkan jumlah total objek dalam direktori yang mencakup objek dihapus, Anda dapat menjalankan perintah PowerShell berikut dari domain yang digabungkan ke instans Windows. Untuk langkah-langkah cara mengatur instans pengelolaan, lihat Mengelola pengguna dan grup di Microsoft AD yang Dikelola AWS.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

Di bawah ini adalah contoh output dari perintah di atas:

```
Count
10000
```

Jika jumlah total di atas jumlah objek yang didukung untuk ukuran direktori yang tercantum dalam catatan di atas, Anda telah melampaui kapasitas direktori Anda.

Di bawah ini adalah pilihan untuk mengatasi gangguan ini:

1. Pembersihan AD
   a. Menghapus objek AD yang tidak diinginkan.
   b. Menghapus objek yang tidak diinginkan dari Keranjang Sampah AD. Ingat bahwa ini merusak dan satu-satunya cara untuk memulihkan objek yang dihapus itu adalah dengan melakukan pemulihan direktori.
   c. Perintah berikut akan menghapus semua objek yang dihapus dari Keranjang Sampah AD.

> **Important**
>
> Gunakan perintah ini dengan hati-hati karena ini merusak dan satu-satunya cara untuk memulihkan objek yang dihapus itu adalah dengan melakukan pemulihan direktori.

```
$DomainInfo = Get-ADDomain
```

```
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
 'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
 { ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
 '*\0ADEL:*') }
ForEach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
 $ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

d. Buka kasus dengan AWS Support untuk meminta AWS Directory Service merebut kembali ruang bebas.

2. Jika tipe direktori Anda adalah Standard Edition Buka kasus dengan AWS Support yang meminta direktori Anda ditingkatkan ke Enterprise Edition. Ini juga akan meningkatkan biaya direktori Anda. Untuk informasi harga, lihat Harga AWS Directory Service.

Di Microsoft AD yang Dikelola AWS, anggota grup Administrator Masa Hidup Objek yang Dihapus yang DidelegasikanAWS memiliki kemampuan untuk memodifikasi atribut `msDS-DeletedObjectLifetime` yang mengatur jumlah waktu dalam hari yang objek dihapus disimpan di Keranjang Sampah AD sebelum mereka menjadi Objek-Daur ulang.

> **Note**
>
> Ini adalah topik lanjutan. Jika dikonfigurasi secara tidak tepat, dapat mengakibatkan kehilangan data. Sebaiknya tinjau terlebih duluAD Recycle Bin: Memahami, Menerapkan, Praktik Terbaik, dan Pemecahan Masalahuntuk mendapatkan pemahaman yang lebih baik tentang proses ini.

Kemampuan untuk mengubah nilai atribut `msDS-DeletedObjectLifetime` ke angka yang lebih rendah dapat membantu memastikan jumlah objek Anda tidak melebihi tingkat yang didukung. Nilai valid terendah atribut ini dapat diatur ke adalah 2 hari. Setelah nilai tersebut melampaui Anda tidak akan lagi dapat memulihkan objek yang dihapus menggunakan Keranjang Sampah AD. Ini akan perlu memulihkan direktori Anda dari snapshot untuk memulihkan objek. Untuk informasi selengkapnya, lihat Snapshot atau pulihkan direktori Anda. Setiap pemulihan dari snapshot dapat mengakibatkan kehilangan data karena mereka adalah titik waktu.

Untuk mengubah Masa Hidup Objek yang Dihapus dari direktori Anda jalankan perintah berikut:

> **Note**
>
> Jika Anda menjalankan perintah seperti adanya, itu akan mengatur nilai atribut Masa Hidup Objek yang Dihapus untuk 30 hari. Jika Anda ingin membuatnya lebih lama atau lebih pendek ganti “30” dengan angka apa pun yang Anda inginkan. Namun, kami merekomendasikan agar Anda tidak mengaturnya lebih dari angka default 180.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
 NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{"msDS-DeletedObjectLifetime" = $DeletedObjectLifetime}
```

Kesalahan ekstensi skema

Berikut ini dapat membantu Anda memecahkan masalah beberapa pesan kesalahan yang mungkin Anda alami ketika memperluas skema untuk direktori Microsoft AD yang Dikelola AWS.

Referral

Kesalahan

> Tambahkan kesalahan pada entri mulai pada baris 1: Referral Kesalahan sisi server adalah: 0x202b Referral dikembalikan dari server. Kesalahan server diperpanjang adalah: 0000202B: RefErr: DSID-0310082F, data 0, 1 titik akses\ tref 1: 'example.com' Jumlah Objek yang Dimodifikasi: 0

Pemecahan Masalah

> Pastikan bahwa semua bidang nama yang dibedakan memiliki nama domain yang benar. Dalam contoh di atas, `DC=example,dc=com` harus diganti dengan `DistinguishedName` yang ditunjukkan oleh cmdlet `Get-ADDomain`.

Tidak dapat membaca file impor

Kesalahan

> Tidak dapat membaca file impor Jumlah Objek yang Dimodifikasi: 0

Pemecahan Masalah

File LDIF yang diimpor kosong (0 byte). Pastikan file yang benar telah diunggah.

Kesalahan sintaks

Kesalahan

Ada kesalahan sintaks dalam file input Gagal pada baris 21. Token terakhir dimulai dengan 'q'. Jumlah Objek yang Dimodifikasi: 0

Pemecahan Masalah

Teks pada baris 21 tidak diformat dengan benar. Huruf pertama dari teks yang tidak valid adalah A. Memperbarui baris 21 dengan sintaks LDIF valid. Untuk informasi selengkapnya tentang format file dalam jumlah besar, lihat Langkah 1: Buat file LDIF Anda.

Atribut atau nilai ada

Kesalahan

Tambahkan kesalahan pada entri mulai pada baris 1: Atribut Atau Nilai Ada Kesalahan sisi server adalah: 0x2083 Nilai yang ditentukan sudah ada. Kesalahan server diperpanjang adalah: 00002083: AtrErr: DSID-03151830, #1:\ t0: 00002083: DSID-03151830, masalah 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain): len 4 Jumlah Objek yang Dimodifikasi: len 4 Jumlah Objek yang 0

Pemecahan Masalah

Perubahan skema telah diterapkan.

Tidak ada atribut tersebut

Kesalahan

Tambahkan kesalahan pada entri mulai pada baris 1: Tidak Ada Atribut Tersebut Kesalahan sisi server adalah: 0x2085 Nilai atribut tidak dapat dihapus karena tidak ada pada objek. Kesalahan server diperpanjang adalah: 00002085: AtrErr: DSID-03152367, #1:\ t0: 00002085: DSID-03152367, masalah 1001 (NO_ATtribut _OR_VAL), data 0, Att 20019 (mayContain) :len 4 Jumlah Objek yang Dimodifikasi: 0

Pemecahan Masalah

File LDIF mencoba untuk menghapus atribut dari kelas, tapi atribut saat ini tidak melekat pada kelas. Perubahan skema mungkin sudah diterapkan.

Kesalahan

Tambahkan kesalahan pada entri mulai pada baris 41: Tidak ada atribut tersebut 0x57 Parameter tidak benar. Kesalahan server yang diperpanjang adalah: 0x208d Objek direktori tidak ditemukan. Kesalahan server diperpanjang adalah: “00000057: LDaperr: DSID-0C090D8A, komentar: Kesalahan dalam operasi konversi atribut, data 0, v2580 “Jumlah Objek Dimodifikasi: 0

Pemecahan Masalah

Atribut yang tercantum pada baris 41 tidak benar. Periksa kembali ejaannya.

Tidak ada objek tersebut

Kesalahan

Tambahkan kesalahan pada entri mulai pada baris 1: Tidak ada Objek Tersebut Kesalahan sisi server adalah: 0x208d Objek direktori tidak ditemukan. Kesalahan server diperpanjang adalah: 0000208D: NameErr: DSID-03100238, masalah 2001 (NO_OBJECT), data 0, pertandingan terbaik dari: 'CN = skema, CN = konfigurasi, DC=example, DC=com' Jumlah Objek yang Dimodifikasi: 0

Pemecahan Masalah

Objek yang direferensikan oleh nama yang dibedakan (DN) tidak ada.

Alasan status pembuatan kepercayaan

Ketika pembuatan kepercayaan gagal, pesan status berisi informasi tambahan. Berikut adalah beberapa bantuan untuk memahami arti pesan tersebut.

Akses ditolak

Akses ditolak ketika mencoba untuk membuat kepercayaan. Kata sandi kepercayaan salah atau pengaturan keamanan domain jarak jauh tidak mengizinkan kepercayaan untuk dikonfigurasi. Untuk menyelesaikan masalah ini, coba hal berikut:

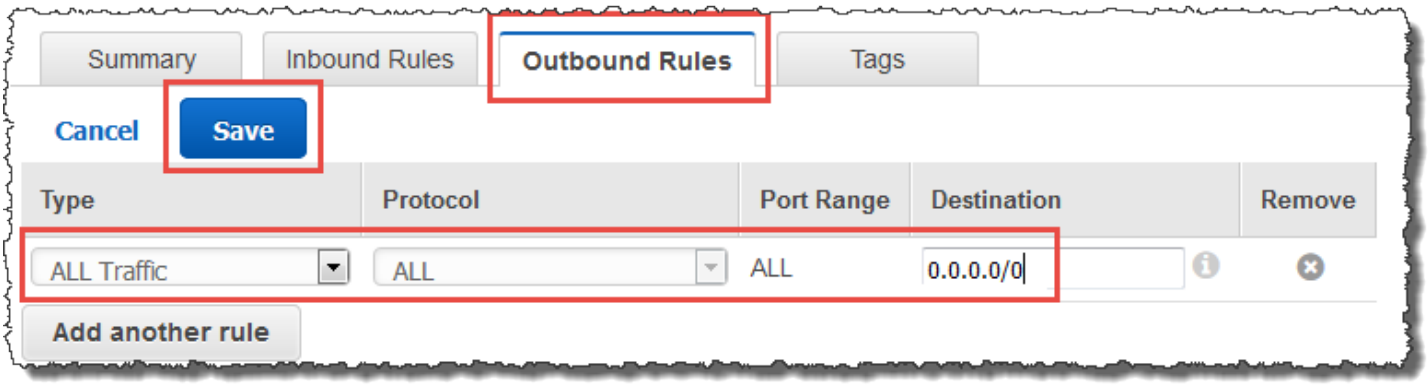
- Iklan Microsoft yang AWS Dikelola Active Directory dan yang dikelola sendiri yang ingin Active Directory Anda buat hubungan kepercayaan, harus memiliki nama Situs Pertama yang sama. Nama Situs Pertama diatur ke`Default-First-Site-Name`. Kesalahan akses ditolak terjadi jika nama-nama ini bervariasi antar domain.
- Verifikasi bahwa Anda menggunakan kata sandi kepercayaan yang sama yang Anda gunakan saat membuat kepercayaan yang sesuai pada domain jarak jauh.
- Verifikasi bahwa pengaturan keamanan domain Anda mengizinkan pembuatan kepercayaan.
- Verifikasi bahwa kebijakan keamanan lokal Anda diatur dengan benar. Periksa secara khusus `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` dan pastikan bahwa itu berisi setidaknya tiga pipe bernama berikut:
  - netlogon
  - samr
  - lsarpc
- Verifikasi bahwa pipa bernama di atas ada sebagai nilai pada kunci NullSessionPipesregistri yang ada di jalur registri HKLM\ SYSTEM\\ services\CurrentControlSet\ Parameters LanmanServer. Nilai-nilai ini harus disisipkan pada baris yang terpisah.

  > **Note**
  >
  > Secara default, `Network access: Named Pipes that can be accessed anonymously` tidak diatur dan akan menampilkan `Not Defined`. Ini adalah normal, sebagai pengendali domain efektif pengaturan default untuk `Network access: Named Pipes that can be accessed anonymously` adalah `netlogon`, `samr`, `lsarpc`.

- Verifikasi Pengaturan Penandatanganan Blok Pesan Server (SMB) berikut dalam Kebijakan Pengontrol Domain Default. Pengaturan ini dapat ditemukan di bawah Konfigurasi Komputer> Pengaturan Windows> Pengaturan Keamanan> Kebijakan Lokal/Opsi Keamanan. Mereka harus cocok dengan pengaturan berikut:
  - Microsoftklien jaringan: Komunikasi tanda tangani secara digital (selalu): Default: Diaktifkan
  - Microsoftklien jaringan: Menandatangani komunikasi secara digital (jika server setuju): Default: Diaktifkan
  - Microsoftserver jaringan: Komunikasi tanda tangani secara digital (selalu): Diaktifkan
  - Microsoftserver jaringan: Menandatangani komunikasi secara digital (jika klien setuju): Default: Diaktifkan

Nama domain yang ditentukan tidak ada atau tidak dapat dihubungi

Untuk mengatasi masalah ini, pastikan pengaturan grup keamanan untuk domain dan daftar kontrol akses (ACL) untuk VPC Anda sudah benar dan Anda telah memasukkan informasi untuk forwarder bersyarat Anda secara akurat. AWS mengkonfigurasi grup keamanan untuk membuka hanya port yang diperlukan untuk komunikasi Active Directory. Dalam konfigurasi default, grup keamanan menerima lalu lintas ke port-port ini dari alamat IP mana pun. Lalu lintas keluar dibatasi untuk grup keamanan. Anda perlu memperbarui aturan keluar pada grup keamanan untuk mengizinkan lalu lintas ke jaringan on-premise Anda. Untuk informasi lebih lanjut tentang persyaratan keamanan, silakan lihatLangkah 2: Siapkan Microsoft AD yang Dikelola AWS.



Jika server DNS untuk jaringan direktori lain menggunakan alamat IP publik (non-RFC 1918), Anda perlu menambahkan rute IP pada direktori dari konsol Directory Services untuk Server DNS. Lihat informasi yang lebih lengkap di Membuat, memverifikasi, atau menghapus hubungan kepercayaan dan Prasyarat.

Internet Assigned Numbers Authority (IANA) telah menyediakan tiga blok dari ruang alamat IP berikut untuk internet pribadi:

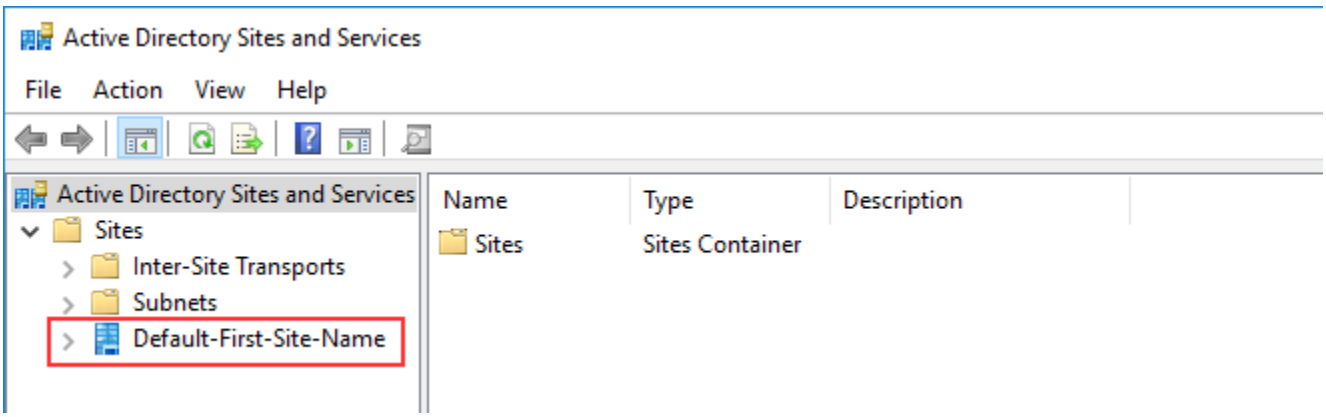
- 10.0.0.0 - 10.255.255.255 (prefiks 10/8)
- 172.16.0.0 - 172.31.255.255 (prefiks 172.16/12)
- 192.168.0.0 - 192.168.255.255 (prefiks 192.168/16)

Untuk informasi selengkapnya, lihat https://tools.ietf.org/html/rfc1918.

Verifikasi bahwa Nama Situs AD Default untuk iklan Microsoft AWS Terkelola cocok dengan Nama Situs AD Default di infrastruktur lokal Anda. Komputer menentukan nama situs menggunakan domain yang di mana komputer adalah anggota, bukan domain pengguna. Mengganti nama situs agar sesuai dengan on-premise terdekat memastikan pencari lokasi DC akan menggunakan pengendali domain

dari situs terdekat. Jika ini tidak menyelesaikan masalah, ada kemungkinan bahwa informasi dari penerus bersyarat yang dibuat sebelumnya telah di-cache, mencegah pembuatan kepercayaan baru. Tunggu beberapa menit, dan kemudian coba buat kepercayaan dan penerus bersyarat lagi.

Untuk informasi selengkapnya tentang cara kerjanya, lihat Domain Locator Across a Forest Trust di Microsoft situs web.



Operasi tidak dapat dilakukan pada domain ini

Untuk mengatasi hal ini, pastikan kedua domain / direktori tidak memiliki nama NETBIOS yang tumpang tindih. Jika domain / direktori memiliki nama NETBIOS yang tumpang tindih, buat kembali salah satu dari mereka dengan nama NETBIOS yang berbeda, dan kemudian coba lagi.

Pembuatan kepercayaan gagal karena kesalahan “Nama domain yang diperlukan dan valid”

Nama DNS hanya bisa berisi karakter abjad (A-Z), karakter numerik (0-9), tanda minus (-), dan titik (.). Karakter titik diperbolehkan hanya ketika mereka digunakan untuk membatasi komponen nama gaya domain. Juga, pertimbangkan hal berikut:

- AWS Microsoft AD yang dikelola tidak mendukung kepercayaan dengan domain label tunggal. Untuk informasi selengkapnya, lihat Microsoftdukungan untuk Domain Label Tunggal.
- Menurut RFC 1123 (https://tools.ietf.org/html/rfc1123), satu-satunya karakter yang dapat digunakan dalam label DNS adalah "A" sampai "Z", "a" sampai "z", "0" sampai "9", and tanda hubung ("-"). Titik [.] juga digunakan dalam nama DNS, tetapi hanya antara label DNS dan pada akhir dari FQDN.
- Menurut RFC 952 (https://tools.ietf.org/html/rfc952), “nama” (Net, Host, Gateway, atau nama Domain) adalah string teks hingga 24 karakter yang diambil dari alfabet (A-Z), angka (0-9),

tanda minus (-), dan titik (.). Perhatikan bahwa titik hanya diperbolehkan ketika berfungsi untuk membatasi komponen “nama gaya domain”.

Untuk informasi selengkapnya, lihat Mematuhi Pembatasan Nama untuk Host dan Domain di Microsoft situs web.

Alat umum untuk menguji kepercayaan

Berikut ini adalah alat yang dapat digunakan untuk memecahkan berbagai masalah terkait kepercayaan.

AWS Alat pemecahan masalah Otomasi Systems Manager

Support Automation Workflows (SAW) memanfaatkan AWS Systems Manager Automation untuk memberi Anda runbook yang telah ditentukan sebelumnya. AWS Directory ServiceAlat AWSSupport- TroubleshootDirectoryTrust runbook membantu Anda mendiagnosis masalah pembuatan kepercayaan umum antara Microsoft AD yang AWS Dikelola dan lokal MicrosoftActive Directory.

DirectoryServicePortTest alat

Alat DirectoryServicePortTestpengujian dapat membantu saat memecahkan masalah pembuatan kepercayaan antara AWS Microsoft AD yang Dikelola dan Direktori Aktif lokal. Sebagai contoh tentang bagaimana alat dapat digunakan, lihat Uji AD Connector Anda.

Alat NETDOM dan NLTEST

Administrator dapat menggunakan alat baris perintah Netdom dan Nltest untuk menemukan, menampilkan, membuat, menghapus, dan mengelola kepercayaan. Alat-alat ini berkomunikasi secara langsung dengan otoritas LSA pada pengendali domain. Untuk contoh tentang cara menggunakan alat ini, lihat Netdom dan NLTEST di situs web. Microsoft

Alat penangkap paket

Anda dapat menggunakan utilitas pengambilan paket Windows bawaan untuk menyelidiki dan memecahkan masalah jaringan potensial. Untuk informasi selengkapnya, lihat Mengambil Jejak Jaringan tanpa menginstal apa pun.

AD Connector

AD Connector adalah gateway direktori yang mana Anda dapat mengalihkan permintaan direktori ke Microsoft Active Directory on-premise Anda tanpa menyimpan informasi apa pun di cloud. AD Connector ada dalam dua ukuran, kecil dan besar. Konektor AD kecil dirancang untuk organisasi yang lebih kecil dan dimaksudkan untuk menangani jumlah operasi per detik yang rendah. Konektor AD besar dirancang untuk organisasi yang lebih besar dan dimaksudkan untuk menangani jumlah operasi per detik sedang hingga tinggi. Anda dapat menyebarkan beban aplikasi di beberapa AD Connector untuk diskalakan dengan kebutuhan performa Anda. Tidak ada batasan pengguna atau koneksi yang ditegakkan.

AD Connector tidak mendukung trust transitif Active Directory. Konektor AD dan domain Active Directory lokal Anda memiliki hubungan 1-ke-1. Artinya, untuk setiap domain lokal, termasuk domain anak di hutan Direktori Aktif yang ingin Anda autentikasi, Anda harus membuat AD Connector yang unik.

> **Note**
>
> AD Connector tidak dapat dibagi dengan akun AWS lain. Jika ini adalah persyaratan, pertimbangkan untuk menggunakan Microsoft AD yang Dikelola AWS untuk Bagikan direktori Anda. AD Connector juga tidak sadar multi-VPC, yang berarti bahwa AWS aplikasi seperti WorkSpacesharus disediakan ke dalam VPC yang sama dengan AD Connector Anda.

Setelah diatur, AD Connector menawarkan manfaat sebagai berikut:

- Pengguna akhir dan administrator TI Anda dapat menggunakan kredensi perusahaan yang ada untuk masuk ke AWS aplikasi seperti, WorkSpaces Amazon, WorkDocs atau Amazon. WorkMail
- Anda dapat mengelola sumber daya AWS seperti instans Amazon EC2 atau bucket Amazon S3 melalui akses berbasis IAM role ke AWS Management Console.
- Anda dapat secara konsisten menegakkan kebijakan keamanan yang ada (seperti kedaluwarsa kata sandi, riwayat kata sandi, dan penguncian akun) baik pengguna maupun administrator IT mengakses sumber daya di infrastruktur lokal atau di Cloud AWS.
- Anda dapat menggunakan AD Connector untuk mengaktifkan autentikasi multi-faktor dengan mengintegrasikan dengan infrastruktur MFA berbasis RADIUS yang ada untuk memberikan lapisan keamanan tambahan saat pengguna mengakses aplikasi AWS.

Lanjutkan membaca topik di bagian ini untuk mempelajari cara menghubungkan ke direktori dan memaksimalkan fitur AD Connector.

Topik

Memulai dengan AD Connector

Dengan AD Connector, Anda dapat terhubung AWS Directory Service ke Active Directory perusahaan yang ada. Saat terhubung ke direktori yang ada, semua data direktori Anda tetap berada di pengontrol domain Anda. AWS Directory Service tidak mereplikasi data direktori Anda.

Topik

Prasyarat AD Connector

Untuk terhubung ke direktori Anda yang sudah ada dengan AD Connector, anda memerlukan hal berikut:

Amazon VPC

Siapkan VPC dengan hal berikut:

- Setidaknya dua subnet. Setiap subnet harus berada di Availability Zone yang berbeda.
- VPC harus terhubung ke jaringan Anda yang sudah ada melalui koneksi jaringan pribadi virtual (VPN) atau AWS Direct Connect.
- VPC harus memiliki penghunian perangkat keras default.

AWS Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar AWS akun Anda, dan dikelola oleh. AWS Mereka memiliki dua adaptor jaringan, `ETH0` dan `ETH1`. `ETH0` adalah adaptor pengelola, dan berada di luar akun Anda. `ETH1` dibuat dalam akun Anda.

Rentang IP pengelola jaringan `ETH0` direktori Anda dipilih secara terprogram untuk memastikan tidak bertentangan dengan VPC tempat direktori Anda di-deploy. Rentang IP ini dapat berupa salah satu pasangan berikut (karena Direktori berjalan di dua subnet):

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

Kami menghindari konflik dengan memeriksa oktet pertama dari `ETH1` CIDR. Jika dimulai dengan 10, maka kami memilih VPC 192.168.0.0/16 dengan subnet 192.168.1.0/24 dan 192.168.2.0/24. Jika oktet pertama adalah yang lain selain 10, kami memilih VPC 10.0.0.0/16 dengan subnet 10.0.1.0/24 dan 10.0.2.0/24.

Algoritma pemilihan tidak mencakup rute pada VPC Anda. Oleh karena itu Anda dapat mengalami konflik IP perutean yang dihasilkan dari skenario ini.

Untuk informasi selengkapnya, lihat topik berikut dalam Panduan Pengguna Amazon VPC:

- Apa itu Amazon VPC?
- Subnet di VPC Anda
- Menambahkan Gerbang Pribadi Virtual Perangkat Keras ke VPC Anda

Untuk informasi selengkapnya AWS Direct Connect, lihat Panduan AWS Direct Connect Pengguna.

yang ada Active Directory

Anda harus terhubung ke jaringan yang ada dengan Active Directory domain.

> **Note**
>
> AD Connector tidak mendukung Domain Label Tunggal.

Tingkat fungsional Active Directory domain ini harus `Windows Server 2003` atau lebih tinggi. AD Connector juga mendukung menghubungkan ke domain yang di-host di instans Amazon EC2.

> **Note**
>
> AD Connector tidak mendukung pengendali domain baca-saja (RODC) jika digunakan dalam kombinasi dengan fitur penggabungan domain Amazon EC2.

Akun layanan

Anda harus memiliki kredensial untuk akun layanan di direktori yang sudah ada yang telah didelegasikan hak istimewa berikut:

- Membaca pengguna dan grup - Diperlukan
- Bergabunglah dengan komputer ke domain - Diperlukan hanya saat menggunakan Seamless Domain Join dan WorkSpaces
- Buat objek komputer - Diperlukan hanya saat menggunakan Seamless Domain Join dan WorkSpaces
- Kata sandi akun layanan harus sesuai dengan persyaratan AWS kata sandi. AWS kata sandi harus:
  - Panjangnya antara 8 dan 128 karakter, inklusif.
  - Berisi setidaknya satu karakter dari tiga dari empat kategori berikut:
    - Huruf kecil (a-z)
    - Huruf besar (A-Z)
    - Angka (0-9)
    - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Untuk informasi selengkapnya, lihat Mendelegasikan hak istimewa ke akun layanan Anda.

> **Note**
>
> AD Connector menggunakan Kerberos untuk autentikasi dan otorisasi aplikasi AWS . LDAP hanya digunakan untuk pencarian objek pengguna dan grup (operasi baca). Dengan transaksi LDAP, tidak ada yang dapat berubah dan kredensial tidak diteruskan dalam teks yang jelas. Otentikasi ditangani oleh layanan AWS internal, yang menggunakan tiket Kerberos untuk melakukan operasi LDAP sebagai pengguna.

Izin pengguna

Semua pengguna Direktori Aktif harus memiliki izin untuk membaca atribut mereka sendiri. Secara spesifik yaitu atribut berikut:

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Secara default, pengguna Direktori Aktif harus memiliki izin untuk membaca atribut-atribut ini. Namun, Administrator dapat mengubah izin ini dari waktu ke waktu sehingga Anda mungkin ingin memverifikasi bahwa pengguna Anda memiliki izin baca ini sebelum menyiapkan AD Connector untuk pertama kalinya.

Alamat IP

Dapatkan alamat IP dari dua server DNS atau pengendali domain di direktori yang ada.

AD Connector memperoleh catatan `_ldap._tcp.<DnsDomainName>` dan `_kerberos._tcp.<DnsDomainName>` SRV dari server ini saat menghubungkan ke direktori Anda, sehingga server ini harus berisi catatan SRV ini. AD Connector mencoba untuk menemukan pengendali domain umum yang akan menyediakan layanan LDAP dan Kerberos, sehingga data SRV ini harus mencakup setidaknya satu pengendali domain umum. Untuk informasi selengkapnya tentang catatan SRV, buka SRV Resource Records di Microsoft. TechNet

Port untuk subnet

Agar AD Connector mengalihkan permintaan direktori ke pengontrol Active Directory domain yang ada, firewall untuk jaringan yang ada harus memiliki port berikut yang terbuka ke CIDR untuk kedua subnet di VPC Amazon Anda.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Autentikasi Kerberos
- TCP/UDP 389 - LDAP

Ini adalah port minimum yang diperlukan sebelum AD Connector dapat terhubung ke direktori Anda. Konfigurasi spesifik Anda mungkin mengharuskan port-port tambahan terbuka.

Jika Anda ingin menggunakan AD Connector dan Amazon WorkSpaces, atribut DisableVLVSupportLDAP harus disetel ke 0 untuk pengontrol domain Anda. Ini adalah pengaturan default untuk pengontrol domain. AD Connector tidak akan dapat menanyakan pengguna di direktori jika atribut DisableVLVSupportLDAP diaktifkan. Ini mencegah AD Connector bekerja dengan Amazon WorkSpaces.

> **Note**
>
> Jika server DNS atau server Pengontrol Domain untuk Active Directory Domain Anda yang ada berada dalam VPC, grup keamanan yang terkait dengan server tersebut harus memiliki port di atas terbuka ke CIDR untuk kedua subnet di VPC.

Untuk persyaratan port tambahan, lihat Persyaratan Port AD dan AD DS pada Microsoft dokumentasi.

Pra-Autentikasi Kerberos

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Untuk petunjuk detail tentang cara mengaktifkan pengaturan ini, lihat Pastikan bahwa Kerberos pra-autentikasi diaktifkan. Untuk informasi umum tentang pengaturan ini, buka Preauthentication on. Microsoft TechNet

Jenis enkripsi

AD Connector mendukung jenis enkripsi berikut ini ketika melakukan autentikasi melalui Kerberos ke pengendali domain Direktori Aktif Anda:

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center prasyarat

Jika Anda berencana untuk menggunakan IAM Identity Center dengan AD Connector, Anda perlu memastikan bahwa berikut ini benar:

- AD Connector Anda disiapkan di akun manajemen AWS organisasi Anda.
- Instance Pusat Identitas IAM Anda berada di Wilayah yang sama tempat AD Connector Anda disiapkan.

Untuk informasi selengkapnya, lihat prasyarat Pusat Identitas IAM di Panduan Pengguna. AWS IAM Identity Center

Prasyarat autentikasi multi-faktor

Untuk mendukung autentikasi multi-faktor dengan direktori AD Connector, Anda memerlukan yang berikut ini:

- Server Remote Authentication Dial-In User Service (RADIUS) di jaringan Anda yang ada yang memiliki dua titik akhir klien. Titik akhir klien RADIUS memiliki persyaratan sebagai berikut:
  - Untuk membuat titik akhir, Anda memerlukan alamat IP server AWS Directory Service . Alamat IP ini dapat diperoleh dari bidang Direktori Alamat IP detail direktori Anda.
  - Kedua titik akhir RADIUS harus menggunakan kode rahasia bersama yang sama.
- Jaringan Anda yang ada harus mengizinkan lalu lintas masuk melalui port server RADIUS default (1812) dari server. AWS Directory Service
- Nama pengguna antara server RADIUS Anda dan direktori Anda harus identik.

Untuk informasi selengkapnya tentang menggunakan AD Connector dengan MFA, lihat Mengaktifkan autentikasi multi-faktor untuk AD Connector.

Mendelegasikan hak istimewa ke akun layanan Anda

Untuk menghubungkan ke direktori Anda, Anda harus memiliki kredensial untuk akun layanan AD Connector di direktori Anda yang telah didelegasikan hak istimewa tertentu. Walaupun anggota grup Admin Domain memiliki hak istimewa yang cukup untuk menghubungkan ke direktori, sebagai praktik terbaik, Anda harus menggunakan akun layanan yang hanya memiliki hak istimewa minimum yang diperlukan untuk menghubungkan ke direktori. Prosedur berikut menunjukkan cara membuat grup baru yang disebut`Connectors`, mendelegasikan hak istimewa yang diperlukan untuk terhubung AWS Directory Service ke grup ini, dan kemudian menambahkan akun layanan baru ke grup ini.

Prosedur ini harus dilakukan pada mesin yang telah digabungkan ke direktori Anda dan memiliki MMC snap-in Pengguna dan Komputer Direktori Aktif terinstal. Anda juga harus masuk sebagai administrator domain.

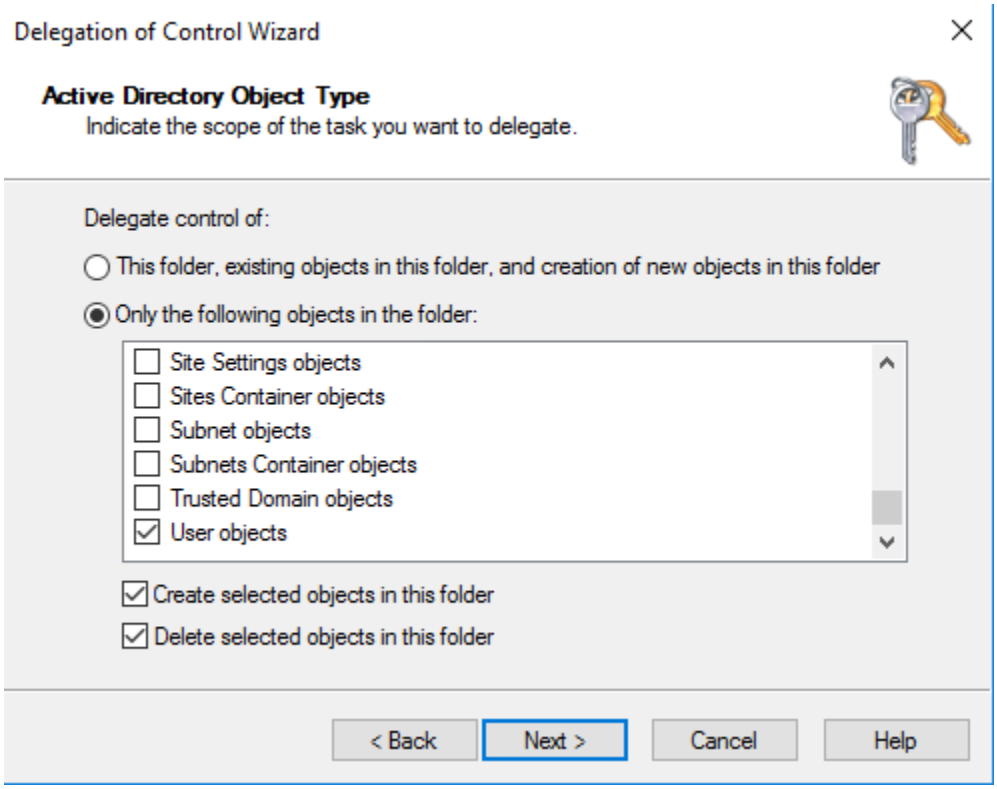
Untuk mendelegasikan hak istimewa ke akun layanan Anda

1. Buka Pengguna dan Komputer Direktori Aktif dan pilih root domain Anda di pohon navigasi.
2. Dalam daftar di panel sebelah kiri, klik kanan Pengguna, pilih Baru, lalu pilih Grup.

3. Di kotak dialog Objek Baru - Grup, masukkan yang berikut ini dan klik OKE.

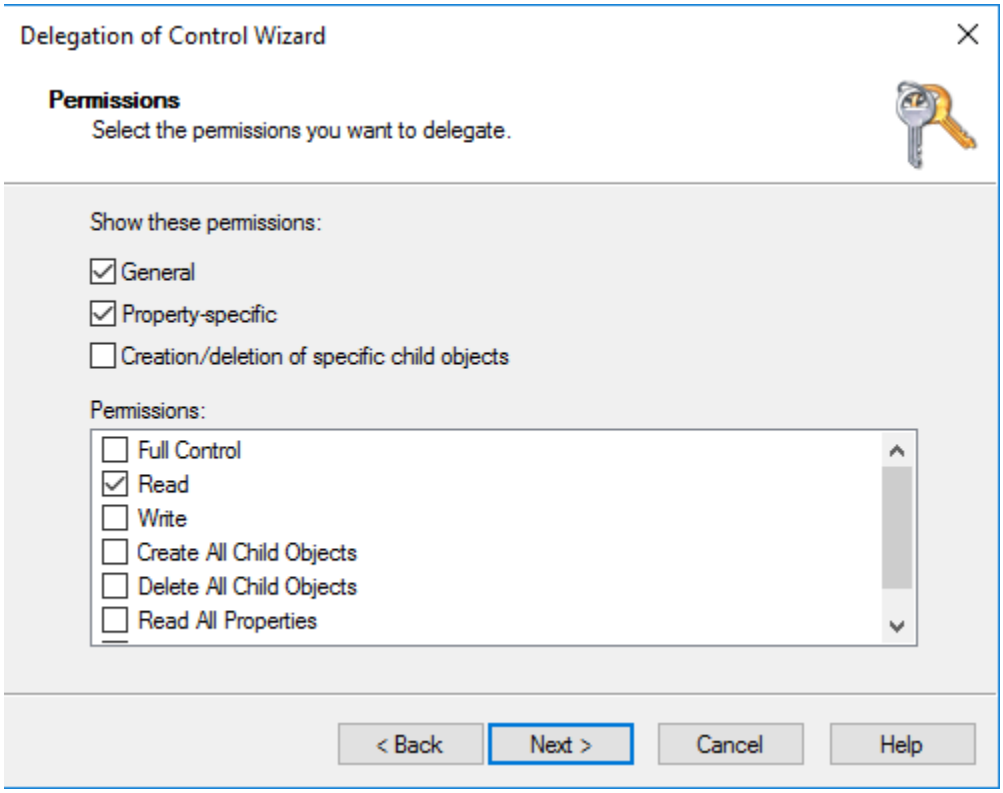
Bidang	Nilai/Pemilihan
Nama grup	`Connectors`
Ruang lingkup kelompok	Global
Jenis grup	Keamanan

4. Di pohon navigasi Pengguna dan Komputer Direktori Aktif, pilih akar domain Anda. Dalam menu, pilih Tindakan, lalu Delegasikan Kontrol. Jika AD Connector Anda terhubung ke Microsoft AD yang AWS Dikelola, Anda tidak akan memiliki akses ke kontrol delegasi di tingkat root domain. Dalam kasus ini, untuk mendelegasikan kontrol, pilih OU di bawah direktori Anda OU Anda tempat objek komputer Anda akan dibuat.
5. Pada halaman Wizard Delegasi Kontrol, klik Selanjutnya, lalu klik Tambahkan.
6. Di kotak dialog Pilih Pengguna, Komputer, atau Grup, masukkan `Connectors` dan klik OKE. Jika ditemukan lebih dari satu objek, pilih grup `Connectors` yang dibuat di atas. Klik Berikutnya.
7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer dan Objek pengguna.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Selanjutnya.



10. Pilih Baca, lalu pilih Selanjutnya.

> **Note**
>
> Jika Anda akan menggunakan Seamless Domain Join atau WorkSpaces, Anda juga harus mengaktifkan izin Tulis sehingga Active Directory dapat membuat objek komputer.



11. Verifikasi informasi pada halaman Wizard Menyelesaikan Delegasi Kontrol, dan klik Selesai.
12. Buat akun pengguna dengan kata sandi yang kuat dan tambahkan pengguna tersebut ke grup `Connectors`. Pengguna ini akan dikenal sebagai akun layanan AD Connector Anda dan karena sekarang menjadi anggota `Connectors` grup, sekarang memiliki hak istimewa yang cukup untuk terhubung AWS Directory Service ke direktori.

Uji AD Connector Anda

Agar AD Connector dapat terhubung ke direktori Anda, firewall untuk jaringan yang ada harus membuat port berikut ini terbuka ke CIDR untuk kedua subnet di VPC. Untuk menguji apakah kondisi ini terpenuhi, lakukan langkah-langkah berikut:

Untuk menguji koneksi

1. Luncurkan instans Windows di VPC dan buat koneksi ke instans melalui RDP. Instans tersebut harus merupakan anggota domain Anda. Langkah-langkah yang tersisa dilakukan pada instans VPC ini.

2. Unduh dan unzip aplikasi DirectoryServicePortTestpengujian. Kode sumber dan file proyek Visual Studio disertakan sehingga Anda dapat memodifikasi aplikasi uji jika diinginkan.

> **Note**
>
> Skrip ini tidak didukung pada Windows Server 2003 atau sistem operasi yang lebih tua.

3. Dari command prompt Windows, jalankan aplikasi uji DirectoryServicePortTest dengan opsi berikut:

> **Note**
>
> Aplikasi DirectoryServicePortTest pengujian hanya dapat digunakan ketika tingkat fungsional domain dan hutan diatur ke Windows Server 2012 R2 dan di bawahnya.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,389" -udp "53,88,389"
```

<domain_name>

Nama domain yang memenuhi syarat. Ini digunakan untuk menguji tingkat fungsional hutan dan domain. Jika Anda mengecualikan nama domain, tingkat fungsional tidak akan diuji.

<server_IP_address>

Alamat IP dari pengendali domain di domain Anda. Port akan diuji terhadap alamat IP ini. Jika Anda mengecualikan alamat IP, port tidak akan diuji.

Aplikasi pengujian ini menentukan apakah port yang diperlukan terbuka dari VPC ke domain Anda, dan juga memverifikasi tingkat fungsional minimum hutan dan domain.

Output akan serupa dengan berikut ini.

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED
```

```
Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
Checking TCP port 88: PASSED
Checking TCP port 389: PASSED

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
Checking UDP port 88: PASSED
Checking UDP port 389: PASSED
```

Berikut ini adalah kode sumber untuk aplikasi DirectoryServicePortTest.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
            if (ParseArgs(args))
```

```
            {
                try
                {
                    if (_domain.Length > 0)
                    {
                        try
                        {
                            TestForestFunctionalLevel();

                            TestDomainFunctionalLevel();
                        }
                        catch (ActiveDirectoryObjectNotFoundException)
                        {
                            Console.WriteLine("The domain {0} could not be found.\n",
_domain);
                        }
                    }

                    if (null != _ipAddr)
                    {
                        if (_tcpPorts.Count > 0)
                        {
                            TestTcpPorts(_tcpPorts);
                        }

                        if (_udpPorts.Count > 0)
                        {
                            TestUdpPorts(_udpPorts);
                        }
                    }
                }
                catch (AuthenticationException ex)
                {
                    Console.WriteLine(ex.Message);
                }
            }
            else
            {
                PrintUsage();
            }

            Console.Write("Press <enter> to continue.");
            Console.ReadLine();
        }
```

```
        static void PrintUsage()
        {
            string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
            Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
        }

        static bool ParseArgs(string[] args)
        {
            bool fReturn = false;
            string ipAddress = "";

            try
            {
                _tcpPorts = new List<int>();
                _udpPorts = new List<int>();

                for (int i = 0; i < args.Length; i++)
                {
                    string arg = args[i];

                    if ("-tcp" == arg | "/tcp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _tcpPorts = ParsePortList(portList);
                    }

                    if ("-udp" == arg | "/udp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _udpPorts = ParsePortList(portList);
                    }

                    if ("-d" == arg | "/d" == arg)
                    {
                        i++;
                        _domain = args[i];
                    }
```

```
                if ("-ip" == arg | "/ip" == arg)
                {
                    i++;
                    ipAddress = args[i];
                }
            }
        }
        catch (ArgumentOutOfRangeException)
        {
            return false;
        }

        if (_domain.Length > 0 || ipAddress.Length > 0)
        {
            fReturn = true;
        }

        if (ipAddress.Length > 0)
        {
            _ipAddr = IPAddress.Parse(ipAddress);
        }

        return fReturn;
    }

    static List<int> ParsePortList(string portList)
    {
        List<int> ports = new List<int>();

        char[] separators = {',', ';', ':'};

        string[] portStrings = portList.Split(separators);
        foreach (string portString in portStrings)
        {
            try
            {
                ports.Add(Convert.ToInt32(portString));
            }
            catch (FormatException)
            {
            }
        }

        return ports;
```

```
        }

        static void TestForestFunctionalLevel()
        {
            Console.WriteLine("Testing forest functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
            Forest forestContext = Forest.GetForest(dirContext);

            Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

            if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static void TestDomainFunctionalLevel()
        {
            Console.WriteLine("Testing domain functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
            Domain domainObject = Domain.GetDomain(dirContext);

            Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

            if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }
```

```
            Console.WriteLine();
        }

        static List<int> TestTcpPorts(List<int> portList)
        {
            Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking TCP port {0}: ", port);

                TcpClient tcpClient = new TcpClient();

                try
                {
                    tcpClient.Connect(_ipAddr, port);

                    tcpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }

        static List<int> TestUdpPorts(List<int> portList)
        {
            Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking UDP port {0}: ", port);
```

```
                UdpClient udpClient = new UdpClient();

                try
                {
                    udpClient.Connect(_ipAddr, port);
                    udpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }
    }
}
```

Membuat AD Connector

Untuk terhubung ke direktori Anda yang sudah ada dengan AD Connector, lakukan langkah-langkah berikut: Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan prasyarat yang diidentifikasi dalam Prasyarat AD Connector.

> **Note**
>
> Anda tidak dapat membuat AD Connector dengan template Cloud Formation.

Untuk menghubungkan dengan AD Connector

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih AD Connector, lalu pilih Selanjutnya.
3. Di halaman Masukkan informasi AD Connector, berikan informasi berikut:

Ukuran direktori

Pilih salah satu opsi ukuran Small atau Large. Untuk informasi selengkapnya tentang ukuran, lihat AD Connector.

Deskripsi direktori

Deskripsi opsional untuk direktori.

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

VPC

VPC untuk direktori.

Subnet

Pilih subnet untuk pengendali domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.

5. Di halaman Hubungkan ke AD, berikan informasi berikut:

Nama DNS direktori

Nama lengkap yang memenuhi syarat untuk direktori Anda, seperti `corp.example.com`.

Direktori nama NetBIOS

Nama pendek untuk direktori Anda, seperti `CORP`.

Alamat IP DNS

Alamat IP setidaknya satu server DNS di direktori yang ada. Server ini harus dapat diakses dari setiap subnet yang ditentukan pada langkah 4. Server ini dapat ditempatkan di luar AWS, selama ada konektivitas jaringan antara subnet yang ditentukan dan alamat IP server DNS.

Nama pengguna akun layanan

Nama pengguna dari pengguna di direktori yang ada. Untuk informasi selengkapnya tentang akun ini, lihat Prasyarat AD Connector.

Kata sandi akun layanan

Kata sandi untuk akun pengguna yang ada. Kata sandi ini peka huruf besar/kecil dan panjangnya harus antara 8 dan 128 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

- Huruf kecil (a-z)
- Huruf besar (A-Z)
- Angka (0-9)
- Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Konfirmasikan kata sandi

Ketik ulang kata sandi untuk akun pengguna yang sudah ada.

6. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Ini akan memerlukan beberapa menit sampai direktori dibuat. Setelah dibuat, nilai Status berubah ke Aktif.

Apa yang dibuat dengan AD Connector Anda

Saat Anda membuat AD Connector, AWS Directory Service secara otomatis membuat dan mengaitkan elastic network interface (ENI) dengan setiap instance AD Connector Anda. Masing-masing ENI ini penting untuk konektivitas antara VPC dan AD AWS Directory Service Connector Anda dan tidak boleh dihapus. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan AWS Directory Service dengan deskripsi: "AWS menciptakan antarmuka jaringan untuk direktori-id direktori". Untuk informasi selengkapnya, lihat Antarmuka Jaringan Elastis di Panduan Pengguna Amazon EC2 untuk Instans Windows.

> **Note**
>
> Instans AD Connector di-deploy di dua Availability Zone di suatu Region secara default dan terhubung ke Amazon Virtual Private Cloud (VPC) Anda. Instans AD Connector yang gagal secara otomatis diganti di Availability Zone yang sama menggunakan alamat IP yang sama.

Saat Anda masuk ke AWS aplikasi atau layanan apa pun yang terintegrasi dengan AD Connector (AWS IAM Identity Center termasuk), aplikasi atau layanan akan meneruskan permintaan autentikasi Anda ke AD Connector yang kemudian meneruskan permintaan ke pengontrol domain di Active Directory yang dikelola sendiri untuk autentikasi. Jika Anda berhasil diautentikasi ke Active Directory yang dikelola sendiri, AD Connector kemudian mengembalikan token otentikasi ke aplikasi atau layanan (mirip dengan token Kerberos). Pada titik ini, Anda sekarang dapat mengakses AWS aplikasi atau layanan.

Cara mengelola AD Connector

Bagian ini mencantumkan semua prosedur untuk mengoperasikan dan memelihara lingkungan AD Connector.

Topik

Mengamankan direktori AD Connector Anda

Bagian ini menjelaskan pertimbangan untuk mengamankan lingkungan AD Connector Anda.

Topik

Memperbarui kredensial akun layanan AD Connector Anda di AWS Directory Service

Kredensial AD Connector yang Anda berikan di AWS Directory Service mewakili akun layanan yang digunakan untuk mengakses direktori on-premise Anda. Anda dapat mengubah kredensial akun layanan di AWS Directory Service dengan melakukan langkah-langkah berikut.

> **Note**
>
> Jika AWS IAM Identity Center diaktifkan untuk direktori, AWS Directory Service harus mentransfer nama utama layanan (SPN) dari akun layanan saat ini ke akun layanan baru.

Jika akun layanan saat ini tidak memiliki izin untuk menghapus SPN atau akun layanan baru tidak memiliki izin untuk menambahkan SPN, Anda akan diminta kredensials akun direktori yang memiliki izin untuk melakukan kedua tindakan tersebut. Kredensial ini hanya digunakan untuk mentransfer SPN dan tidak disimpan oleh layanan.

Untuk memperbarui kredensial akun layanan AD Connector Anda di AWS Directory Service

1. Di panel navigasi AWS Directory Servicekonsol, di bawah Active Directory, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, gulir ke bawah ke bagian Kredensial akun Layanan.
4. Di bagian Kredensial akun layanan, pilih Perbarui.
5. Di kotak dialog Perbarui kredensi akun layanan, ketik nama pengguna dan kata sandi akun layanan. Masukkan kembali kata sandi untuk mengonfirmasinya dan kemudian pilih Perbarui.

Mengaktifkan autentikasi multi-faktor untuk AD Connector

Anda dapat mengaktifkan autentikasi multi-faktor untuk AD Connector bila Anda memiliki Direktori Aktif yang berjalan on-premise atau dalam instans EC2. Untuk informasi lebih lanjut tentang menggunakan autentikasi multi-faktor dengan AWS Directory Service, lihat Prasyarat AD Connector.

Note

Autentikasi multi-faktor tidak tersedia untuk Simple AD. Namun, autentikasi multi-faktor (MFA) dapat diaktifkan untuk direktori Microsoft AD yang Dikelola AWS. Untuk informasi selengkapnya, lihat Mengaktifkan autentikasi multi-faktor untuk Microsoft AD yang Dikelola AWS.

Untuk mengaktifkan autentikasi multi-faktor untuk AD Connector

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi multi-faktor, pilih Tindakan, lalu pilih Aktifkan.
5. Pada halaman Aktifkan multi-factor authentication (MFA), berikan nilai berikut:

Label tampilan

Berikan nama label.

Nama DNS server RADIUS atau alamat IP

Alamat IP titik akhir server RADIUS, atau alamat IP penyeimbang beban server RADIUS. Anda dapat memasukkan beberapa alamat IP dengan memisahkannya dengan koma (misalnya, `192.0.0.0,192.0.0.12`).

> **Note**
>
> RADIUS MFA hanya berlaku untuk mengautentikasi akses keAWS Management Console, atau ke aplikasi dan layanan Amazon Enterprise seperti, WorkSpaces Amazon, atau Amazon QuickSight Chime. Ini tidak menyediakan autentikasi multi-faktor (MFA) ke beban kerja Windows yang berjalan pada instans EC2, atau untuk masuk ke instans EC2. AWS Directory Service tidak mendukung autentikasi Tantangan/Tanggapan RADIUS.
> Pengguna harus memiliki kode MFA mereka pada saat mereka memasukkan nama pengguna dan kata sandi mereka. Atau, Anda harus menggunakan solusi yang melakukan MFA out-of-band seperti verifikasi teks SMS untuk pengguna. Dalam solusi out-of-band MFA, Anda harus memastikan bahwa Anda menetapkan nilai batas waktu RADIUS dengan tepat untuk solusi Anda. Saat menggunakan solusi out-of-band MFA, halaman masuk akan meminta pengguna untuk kode MFA. Dalam hal ini, praktik terbaik adalah bagi pengguna untuk memasukkan kata sandi mereka di bidang kata sandi dan bidang autentikasi multi-faktor (MFA).

Pelabuhan

Port yang digunakan oleh server RADIUS Anda untuk komunikasi. Jaringan on-premise Anda harus mengizinkan lalu lintas masuk melalui port server RADIUS default (UDP:1812) dari server AWS Directory Service.

Kode rahasia bersama

Kode rahasia bersama yang ditentukan ketika titik akhir RADIUS Anda dibuat.

Konfirmasikan kode rahasia bersama

Konfirmasi kode rahasia bersama untuk titik akhir RADIUS Anda.

Protokol

Pilih protokol yang ditentukan saat titik akhir RADIUS Anda dibuat.

Batas waktu server (dalam hitungan detik)

Jumlah waktu, dalam detik, untuk menunggu server RADIUS menanggapi. Ini harus berupa nilai antara 1 dan 50.

Permintaan Max RADIUS mencoba ulang

Berapa kali komunikasi dengan server RADIUS dicoba. Ini harus berupa nilai antara 0 dan 10.

Autentikasi multi-faktor tersedia ketika Status RADIUS berubah ke Diaktifkan.

6. Pilih Aktifkan.

Aktifkan LDAPS sisi klien menggunakan AD Connector

Dukungan LDAPS sisi klien di AD Connector mengenkripsi komunikasi antara Microsoft Active Directory (AD) dan aplikasi AWS. Contoh aplikasi tersebut meliputi WorkSpaces,AWS IAM Identity CenterAmazon QuickSight, dan Amazon Chime. Enkripsi ini membantu Anda melindungi data identitas organisasi dengan lebih baik dan memenuhi persyaratan keamanan Anda.

Topik

- Prasyarat
- Aktifkan LDAPS sisi klien
- Mengelola LDAPS sisi klien

Prasyarat

Sebelum Anda mengaktifkan LDAPS sisi klien, Anda harus memenuhi persyaratan berikut.

Topik

- Men-deploy sertifikat server di Direktori Aktif

- Persyaratan sertifikat CA
- Persyaratan jaringan

Men-deploy sertifikat server di Direktori Aktif

Untuk mengaktifkan LDAPS sisi klien, Anda perlu untuk mendapatkan dan menginstal sertifikat server untuk setiap pengendali domain di Direktori Aktif. Sertifikat ini akan digunakan oleh layanan LDAP untuk mendengarkan dan secara otomatis menerima koneksi SSL dari klien LDAP. Anda dapat menggunakan sertifikat SSL yang dikeluarkan oleh deployment Active Directory Certificate Services (ADCS) atau dibeli dari penerbit komersial. Untuk informasi lebih lanjut tentang persyaratan sertifikat server Direktori Aktif, lihat LDAP melalui Sertifikat SSL (LDAPS) di situs web Microsoft.

Persyaratan sertifikat CA

Sertifikat otoritas sertifikat (CA), yang mewakili penerbit sertifikat server Anda, diperlukan untuk operasi LDAPS sisi klien. Sertifikat CA cocok dengan sertifikat server yang disajikan oleh pengendali domain Direktori Aktif Anda untuk mengenkripsi komunikasi LDAP. Perhatikan persyaratan sertifikat CA berikut:

- Untuk mendaftarkan sertifikat, harus lebih dari 90 hari dari kedaluwarsa.
- Sertifikat harus dalam format Privacy Enhanced Mail (PEM). Jika mengekspor sertifikat CA dari dalam Direktori Aktif, pilih base64 encoded X.509 (.CER) sebagai format file ekspor.
- Maksimum lima (5) sertifikat CA dapat disimpan per direktori AD Connector.
- Sertifikat yang menggunakan algoritma tanda tangan RSASSA-PSS tidak didukung.

Persyaratan jaringan

Lalu lintas LDAP aplikasi AWS akan berjalan secara eksklusif pada TCP port 636, tanpa fallback ke LDAP port 389. Namun, komunikasi Windows LDAP yang mendukung replikasi, kepercayaan, dan banyak lagi akan terus menggunakan LDAP port 389 dengan keamanan native Windows. Konfigurasikan grup keamanan AWS dan network firewall untuk mengizinkan komunikasi TCP pada port 636 di AD Connector (outbound) dan Direktori Aktif yang dikelola sendiri (inbound).

Aktifkan LDAPS sisi klien

Untuk mengaktifkan LDAPS sisi klien, Anda mengimpor sertifikat otoritas sertifikat (CA) ke AD Connector, dan kemudian mengaktifkan LDAPS di direktori Anda. Setelah mengaktifkan, semua lalu

lintas LDAP antara aplikasi AWS dan Direktori Aktif Anda akan mengalir dengan enkripsi saluran Lapisan Socket Aman (SSL).

Anda dapat menggunakan dua metode yang berbeda untuk mengaktifkan LDAPS sisi klien untuk direktori Anda. Anda dapat menggunakan metode AWS Management Console atau metode AWS CLI.

Topik

Langkah 1: Daftarkan sertifikat diAWS Directory Service

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat di AWS Directory Service.

Metode 1: Untuk mendaftarkan sertifikatAWS Directory Service(AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih menu Tindakan, lalu pilih Mendaftarkan sertifikat.
5. Di kotak dialog Daftarkan sertifikat CA, pilih Telusuri, lalu pilih sertifikat dan pilih Buka.
6. Pilih Daftarkan sertifikat.

Metode 2: Untuk mendaftarkan sertifikatAWS Directory Service(AWS CLI)

- Jalankan perintah berikut. Untuk data sertifikat, arahkan ke lokasi file sertifikat CA Anda. ID sertifikat akan diberikan dalam tanggapan.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Langkah 2: Periksa status registrasi

Untuk melihat status pendaftaran sertifikat atau daftar sertifikat terdaftar, gunakan salah satu metode berikut:

Metode 1: Untuk memeriksa status pendaftaran sertifikat diAWS Directory Service(AWS Management Console)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Meninjau status pendaftaran sertifikat saat ini yang ditampilkan di bawah kolom Status pendaftaran. Ketika nilai status pendaftaran berubah menjadi Registered, sertifikat Anda telah berhasil didaftarkan.

Metode 2: Untuk memeriksa status pendaftaran sertifikat diAWS Directory Service(AWS CLI)

- Jalankan perintah berikut. Jika nilai status mengembalikan `Registered`, sertifikat Anda telah berhasil didaftarkan.

```
aws ds list-certificates --directory-id your_directory_id
```

Langkah 3: Aktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk mengaktifkan LDAPS sisi klien di AWS Directory Service.

> **Note**
>
> Anda harus berhasil mendaftarkan setidaknya satu sertifikat sebelum Anda dapat mengaktifkan LDAPS sisi klien.

Metode 1: Untuk mengaktifkan LDAPS sisi klien diAWS Directory Service(AWS Management Console)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Pilih Aktifkan. Jika opsi ini tidak tersedia, verifikasi bahwa sertifikat yang valid telah berhasil terdaftar, dan kemudian coba lagi.
3. Di kotak dialog Aktifkan LDAPS sisi klien, pilih Aktifkan.

Metode 2: Untuk mengaktifkan LDAPS sisi klien diAWS Directory Service(AWS CLI)

- Jalankan perintah berikut.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Langkah 4: Periksa status LDAPS

Gunakan salah satu metode berikut untuk memeriksa status LDAPS di AWS Directory Service.

Metode 1: Untuk memeriksa status LDAPS diAWS Directory Service(AWS Management Console)

1. Buka bagian LDAPS sisi klien pada halaman Detail direktori.
2. Jika nilai status ditampilkan sebagai Diaktifkan, LDAPS telah berhasil dikonfigurasi.

Metode 2: Untuk memeriksa status LDAPS diAWS Directory Service(AWS CLI)

- Jalankan perintah berikut. Jika nilai status mengembalikan `Enabled`, LDAPS telah berhasil dikonfigurasi.

```
aws ds describe-ldaps-settings -directory-id your_directory_id
```

Mengelola LDAPS sisi klien

Gunakan perintah ini untuk mengelola konfigurasi LDAPS Anda.

Anda dapat menggunakan dua metode yang berbeda untuk mengelola pengaturan LDAPS sisi klien. Anda dapat menggunakan metode AWS Management Console atau metode AWS CLI.

Melihat detail sertifikat

Gunakan salah satu metode berikut untuk melihat ketika sertifikat diatur untuk kedaluwarsa.

Metode 1: Untuk melihat rincian sertifikat diAWS Directory Service(AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.

4. Di bagian LDAPS sisi klien, di bawah Sertifikat CA, informasi tentang sertifikat akan ditampilkan.

Metode 2: Untuk melihat rincian sertifikat diAWS Directory Service(AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Membatalkan pendaftaran sertifikat

Gunakan salah satu metode berikut untuk membatalkan pendaftaran sertifikat.

> **Note**
>
> Jika hanya satu sertifikat yang terdaftar, Anda harus terlebih dahulu menonaktifkan LDAPS sebelum Anda dapat membatalkan pendaftaran sertifikat.

Metode 1: Untuk membatalkan pendaftaran sertifikat diAWS Directory Service(AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih Tindakan, lalu pilih Membatalkan pendaftaran sertifikat.
5. Di kotak dialog Membatalkan pendaftaran sertifikat CA, pilih Batalkan pendaftaran.

Metode 2: Untuk membatalkan pendaftaran sertifikat diAWS Directory Service(AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Menonaktifkan LDAPS sisi klien

Gunakan salah satu metode berikut untuk menonaktifkan LDAPS sisi klien.

Metode 1: Untuk menonaktifkan LDAPS sisi klien diAWS Directory Service(AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian LDAPS sisi klien, pilih Nonaktifkan.
5. Di kotak dialog Nonaktifkan LDAPS sisi klien, pilih Nonaktifkan.

Metode 2: Untuk menonaktifkan LDAPS sisi klien diAWS Directory Service(AWS CLI)

- Jalankan perintah berikut.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Aktifkan autentikasi mTLS di AD Connector untuk digunakan dengan kartu pintar

Anda dapat menggunakan autentikasi mutual Transport Layer Security (mTLS) berbasis sertifikat dengan kartu pintar untuk mengautentikasi pengguna ke Amazon WorkSpaces melalui Active Directory (AD) dan AD Connector yang dikelola sendiri. Saat diaktifkan, pengguna memilih kartu pintar mereka di layar WorkSpaces login dan memasukkan PIN untuk mengautentikasi, alih-alih menggunakan nama pengguna dan kata sandi. Dari sana, desktop virtual Windows atau Linux menggunakan kartu pintar untuk mengautentikasi ke AD dari OS desktop asli.

> **Note**
>
> Otentikasi kartu pintar di AD Connector hanya tersedia di berikut ini Wilayah AWS, dan hanya dengan WorkSpaces. AWS Aplikasi lain tidak didukung saat ini.
>
> - AS Timur (Virginia Utara)
> - US West (Oregon)
> - Asia Pasifik (Sydney)
> - Asia Pasifik (Tokyo)

- Eropa (Irlandia)
- AWS GovCloud (AS-Barat)

Topik

- Prasyarat
- Aktifkan otentikasi kartu pintar
- Mengelola pengaturan otentikasi kartu pintar

Prasyarat

Untuk mengaktifkan autentikasi Mutual Transport Layer Security (mTLS) berbasis sertifikat menggunakan kartu pintar untuk WorkSpaces klien Amazon, Anda memerlukan infrastruktur kartu pintar operasional yang terintegrasi dengan pengelolaan sendiri. Active Directory Untuk informasi selengkapnya tentang cara mengatur otentikasi kartu pintar dengan Amazon WorkSpaces danActive Directory, lihat Panduan WorkSpaces Administrasi Amazon.

Sebelum Anda mengaktifkan otentikasi kartu pintar untuk WorkSpaces, harap tinjau pertimbangan berikut:

- Persyaratan sertifikat CA
- Persyaratan sertifikat pengguna
- Proses pengecekan pencabutan sertifikat
- Pertimbangan lainnya

Persyaratan sertifikat CA

AD Connector memerlukan sertifikat otoritas sertifikasi (CA), yang mewakili penerbit sertifikat pengguna Anda, untuk autentikasi kartu pintar. AD Connector mencocokkan sertifikat CA dengan sertifikat yang ditampilkan oleh pengguna Anda dengan kartu pintar mereka. Perhatikan persyaratan sertifikat CA berikut:

- Sebelum Anda dapat mendaftarkan sertifikat CA, harus lebih dari 90 hari dari kedaluwarsa.
- Sertifikat CA harus dalam format Privacy-Enhanced Mail (PEM). Jika Anda mengekspor sertifikat CA dari dalam Direktori Aktif, pilih base64 encoded X.509 (.CER) sebagai format file ekspor.

- Semua sertifikat CA root dan perantara yang terangkai dari CA penerbit sampai sertifikat pengguna harus diunggah agar autentikasi kartu pintar berhasil.
- Maksimum 100 sertifikat CA dapat disimpan per direktori AD Connector
- AD Connector tidak mendukung algoritma tanda tangan RSASSA-PSS untuk sertifikat CA.
- Verifikasi Layanan Propagasi Sertifikat diatur ke Otomatis dan berjalan.

Persyaratan sertifikat pengguna

Berikut ini adalah beberapa persyaratan untuk sertifikat pengguna:

- Sertifikat kartu pintar pengguna memiliki Nama Alternatif Subjek (SAN) dari pengguna userPrincipalName (UPN).
- Sertifikat kartu pintar pengguna memiliki Penggunaan Kunci yang Ditingkatkan sebagai log-on kartu pintar (1.3.6.1.4.1.311.20.2.2) Otentikasi Klien (1.3.6.1.5.5.7.3.2).
- Informasi Protokol Status Sertifikat Online (OCSP) untuk sertifikat kartu pintar pengguna harus berupa Metode Akses = Protokol Status Sertifikat On-line (1.3.6.1.5.5.7.48.1) di Akses Informasi Otoritas.

Untuk informasi selengkapnya tentang AD Connector dan persyaratan autentikasi kartu pintar, lihat Persyaratan di Panduan WorkSpaces Administrasi Amazon. Untuk membantu mengatasi WorkSpaces masalah Amazon, seperti masuk ke, mengatur ulang kata sandi WorkSpaces, atau menyambungkan ke WorkSpaces, lihat Memecahkan WorkSpaces masalah klien di Panduan Pengguna Amazon. WorkSpaces

Proses pengecekan pencabutan sertifikat

Untuk melakukan autentikasi kartu pintar, AD Connector harus memeriksa status pencabutan sertifikat pengguna menggunakan Online Certificate Status Protocol (OCSP). Untuk melakukan pengecekan pencabutan sertifikat, URL penjawab OCSP harus dapat diakses internet. Jika menggunakan nama DNS, URL penjawab OCSP harus menggunakan domain tingkat atas yang ditemukan di Basis Data Zona Root Internet Assigned Numbers Auhtority (IANA).

Pemeriksaan pencabutan sertifikat AD Connector menggunakan proses berikut ini:

- AD Connector harus memeriksa ekstensi Authority Information Access (AIA) di sertifikat pengguna untuk URL penjawab OCSP, lalu AD Connector menggunakan URL tersebut untuk memeriksa pencabutan.

- Jika AD Connector tidak dapat menyelesaikan URL yang ditemukan di ekstensi AIA sertifikat pengguna, atau menemukan URL penjawab OCSP di sertifikat pengguna, AD Connector menggunakan URL OCSP opsional yang disediakan selama pendaftaran sertifikat CA root.

  Jika URL di ekstensi AIA sertifikat pengguna terselesaikan tapi tidak responsif, maka autentikasi pengguna gagal.
- Jika URL penjawab OCSP yang disediakan selama pendaftaran sertifikat CA root tidak dapat diselesaikan, tidak responsif, atau tidak ada URL penjawab OCSP yang disediakan, autentikasi pengguna gagal.
- Server OCSP harus sesuai dengan RFC 6960. Selain itu, server OCSP harus mendukung permintaan menggunakan metode GET untuk permintaan yang kurang dari atau sama dengan 255 byte secara total.

> **Note**
>
> AD Connector memerlukan URL HTTP untuk URL penjawab OCSP.

Pertimbangan lainnya

Sebelum mengaktifkan autentikasi kartu pintar di AD Connector, pertimbangkan item berikut ini:

- AD Connector menggunakan autentikasi Transport Layer Security berbasis sertifikat (mutual TLS) untuk mengautentikasi pengguna ke Direktori Aktif menggunakan sertifikat kartu pintar berbasis perangkat keras atau perangkat lunak. Hanya kartu akses umum (CAC) dan kartu verifikasi identitas pribadi (PIV) yang didukung saat ini. Jenis lain dari perangkat keras atau kartu pintar berbasis perangkat lunak mungkin berfungsi tetapi belum diuji untuk digunakan dengan Protokol Streaming. WorkSpaces
- Otentikasi kartu pintar menggantikan otentikasi nama pengguna dan kata sandi ke. WorkSpaces

  Jika Anda memiliki AWS aplikasi lain yang dikonfigurasi di direktori AD Connector Anda dengan otentikasi kartu pintar diaktifkan, aplikasi tersebut masih menampilkan layar input nama pengguna dan kata sandi.
- Mengaktifkan autentikasi kartu pintar membatasi panjang sesi pengguna ke maksimum seumur hidup untuk tiket layanan Kerberos. Anda dapat mengkonfigurasi pengaturan ini menggunakan Kebijakan Grup, dan diatur ke 10 jam secara default. Untuk informasi lebih lanjut tentang pengaturan ini, lihat Dokumentasi Microsoft.

- Jenis enkripsi Kerberos yang didukung oleh akun layanan AD Connector harus sesuai dengan setiap jenis enkripsi Kerberos yang didukung pengontrol domain.

Aktifkan otentikasi kartu pintar

Untuk mengaktifkan otentikasi kartu pintar WorkSpaces di AD Connector, pertama-tama Anda harus mengimpor sertifikat otoritas sertifikat (CA) ke AD Connector. Anda dapat mengimpor sertifikat CA ke AD Connector menggunakan AWS Directory Service konsol, API, atau CLI. Gunakan langkah-langkah berikut untuk mengimpor sertifikat CA Anda dan selanjutnya mengaktifkan otentikasi kartu pintar.

Topik

Langkah 1: Aktifkan delegasi terbatas Kerberos untuk akun layanan AD Connector

Untuk menggunakan otentikasi kartu pintar dengan AD Connector, Anda harus mengaktifkan Kerberos Constrained Delegation (KCD) untuk akun AD Connector Service ke layanan LDAP di direktori AD yang dikelola sendiri.

Kerberos Constrained Delegation adalah sebuah fitur di Windows Server. Fitur ini mengizinkan administrator untuk menentukan dan memberlakukkan batasan kepercayaan aplikasi dengan membatasi lingkup tempat layanan aplikasi dapat bertindak atas nama pengguna. Untuk informasi selengkapnya, lihat Delegasi yang dibatasi Kerberos.

> **Note**
>
> Kerberos Constrained Delegation (KCD) memerlukan bagian nama pengguna dari akun layanan AD Connector agar sesuai dengan SAM dari pengguna yang sama. AccountName SAM AccountName dibatasi hingga 20 karakter. sM AccountName adalah atribut Microsoft Active Directory yang digunakan sebagai nama masuk untuk versi klien dan server Windows sebelumnya.

1. Gunakan `SetSpn` perintah untuk menetapkan Service Principal Name (SPN) untuk akun layanan AD Connector di AD yang dikelola sendiri. Hal ini mengizinkan akun layanan untuk konfigurasi delegasi.

   SPN dapat berupa kombinasi layanan atau nama tetapi bukan duplikat SPN yang ada. `-s` memeriksa adanya duplikat.

   ```
   setspn -s my/spn service_account
   ```
2. Di Pengguna dan Komputer AD, buka menu konteks (klik kanan) dan pilih akun layanan AD Connector dan pilih Properties.
3. Pilih tab Delegasi.
4. Pilih Percayai pengguna ini untuk delegasi ke layanan tertentu saja dan Gunakan opsi protokol otentikasi apa pun.
5. Pilih Tambahkan lalu Pengguna atau Komputer untuk menemukan pengendali domain.
6. Pilih OKE untuk menampilkan daftar layanan tersedia yang digunakan untuk delegasi.
7. Pilih jenis layanan ldap dan pilih OK.
8. Pilih OK lagi untuk menyimpan konfigurasi.
9. Ulangi proses ini untuk pengontrol domain lain di Direktori Aktif. Atau Anda dapat mengotomatiskan proses menggunakan PowerShell.

Langkah 2: Daftarkan sertifikat CA di AD Connector

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat CA untuk direktori AD Connector Anda.

Metode 1: Untuk mendaftarkan sertifikat CA Anda di AD Connector (AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi kartu pintar, pilih Tindakan, lalu pilih Daftar sertifikat.
5. Dalam kotak dialog Daftarkan sertifikat, pilih Pilih file, lalu pilih sertifikat dan pilih Buka. Anda dapat memilih untuk melakukan pengecekan pencabutan sertifikat ini dengan memberikan URL responder Online Certificate Status Protocol (OCSP). Untuk informasi lebih lanjut tentang OCSP, lihatProses pengecekan pencabutan sertifikat.

6. Pilih Daftarkan sertifikat. Ketika Anda melihat perubahan status sertifikat menjadi Terdaftar, proses pendaftaran telah selesai dengan sukses.

Metode 2: Untuk mendaftarkan sertifikat CA Anda di AD Connector (AWS CLI)

- Jalankan perintah berikut. Untuk data sertifikat, arahkan ke lokasi file sertifikat CA Anda. Untuk memberikan alamat penjawab OCSP sekunder, gunakan objek `ClientCertAuthSettings` opsional.

```
aws ds register-certificate --directory-id your_directory_id --certificate-
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings
 OCSPUrl=http://your_OCSP_address
```

Jika berhasil, respons memberikan ID sertifikat. Anda juga dapat memverifikasi sertifikat CA Anda terdaftar berhasil dengan menjalankan perintah CLI berikut:

```
aws ds list-certificates --directory-id your_directory_id
```

Jika nilai status mengembalikan `Registered`, Anda telah berhasil mendaftarkan sertifikat Anda.

Langkah 3: Aktifkan otentikasi kartu pintar untuk AWS aplikasi dan layanan yang didukung

Gunakan salah satu metode berikut untuk mendaftarkan sertifikat CA untuk direktori AD Connector Anda.

Metode 1: Untuk mengaktifkan otentikasi kartu pintar di AD Connector ()AWS Management Console

1. Arahkan ke bagian otentikasi kartu pintar di halaman Detail direktori, dan pilih Aktifkan. Jika opsi ini tidak tersedia, verifikasi bahwa sertifikat yang valid telah berhasil terdaftar, dan kemudian coba lagi.
2. Dalam kotak dialog Aktifkan otentikasi kartu pintar, pilih Aktifkan.

Metode 2: Untuk mengaktifkan otentikasi kartu pintar di AD Connector ()AWS CLI

- Jalankan perintah berikut.

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Jika berhasil, AD Connector akan mengembalikan respons `HTTP 200` dengan tubuh HTTP kosong.

Mengelola pengaturan otentikasi kartu pintar

Anda dapat menggunakan dua metode berbeda untuk mengelola pengaturan kartu pintar. Anda dapat menggunakan AWS Management Console metode atau AWS CLI metode.

Topik

- Melihat detail sertifikat
- Membatalkan pendaftaran sertifikat
- Nonaktifkan otentikasi kartu pintar

Melihat detail sertifikat

Gunakan salah satu metode berikut untuk melihat ketika sertifikat diatur untuk kedaluwarsa.

Metode 1: Untuk melihat detail sertifikat di AWS Directory Service (AWS Management Console)

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi kartu pintar, di bawah sertifikat CA, pilih ID sertifikat untuk menampilkan detail tentang sertifikat tersebut.

Metode 2: Untuk melihat detail sertifikat di AWS Directory Service (AWS CLI)

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Membatalkan pendaftaran sertifikat

Gunakan salah satu metode berikut untuk membatalkan pendaftaran sertifikat.

> **Note**
>
> Jika hanya satu sertifikat yang terdaftar, Anda harus menonaktifkan otentikasi kartu pintar terlebih dahulu sebelum Anda dapat membatalkan pendaftaran sertifikat.

Metode 1: Untuk membatalkan pendaftaran sertifikat di () AWS Directory ServiceAWS Management Console

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian Autentikasi kartu pintar, di bawah sertifikat CA, pilih sertifikat yang ingin Anda deregister, pilih Tindakan, lalu pilih Deregister Certificate.

   > **Important**
   >
   > Pastikan sertifikat yang akan Anda deregister tidak aktif atau saat ini digunakan sebagai bagian dari rantai sertifikat CA untuk otentikasi kartu pintar.

5. Di kotak dialog Membatalkan pendaftaran sertifikat CA, pilih Batalkan pendaftaran.

Metode 2: Untuk membatalkan pendaftaran sertifikat di () AWS Directory ServiceAWS CLI

- Jalankan perintah berikut. Untuk ID sertifikat, gunakan pengidentifikasi yang dikembalikan oleh `register-certificate` atau `list-certificates`.

  ```
  aws ds deregister-certificate --directory-id your_directory_id --certificate-id your_cert_id
  ```

Nonaktifkan otentikasi kartu pintar

Gunakan salah satu metode berikut untuk menonaktifkan otentikasi kartu pintar.

Metode 1: Untuk menonaktifkan otentikasi kartu pintar di AWS Directory Service ()AWS Management Console

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pilih tautan ID direktori untuk direktori AD Connector Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & keamanan.
4. Di bagian otentikasi kartu pintar, pilih Nonaktifkan.
5. Dalam kotak dialog Nonaktifkan otentikasi kartu pintar, pilih Nonaktifkan.

Metode 2: Untuk menonaktifkan otentikasi kartu pintar di AWS Directory Service ()AWS CLI

- Jalankan perintah berikut.

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Siapkan AWS Private CA Konektor untuk AD

Anda dapat mengintegrasikan Active Directory (AD) yang dikelola sendiri dengan AWS Private Certificate Authority (CA) dengan AD Connector untuk menerbitkan dan mengelola sertifikat bagi pengguna, grup, dan mesin yang bergabung dengan domain AD Anda. AWS Private CA Connector for AD memungkinkan Anda menggunakan pengganti AWS Private CA drop-in yang dikelola sepenuhnya untuk CA perusahaan yang dikelola sendiri tanpa perlu menyebarkan, menambal, atau memperbarui agen lokal atau server proxy.

Anda dapat mengatur AWS Private CA integrasi dengan direktori Anda melalui konsol Directory Service, AWS Private CA Connector for AD console, atau dengan memanggil `CreateTemplate`API. Untuk menyiapkan integrasi Private CA melalui konsol AWS Private CA Connector for Active Directory, lihat AWS Private CA Connector for Active Directory. Lihat di bawah untuk langkah-langkah tentang cara mengatur integrasi ini dari AWS Directory Service konsol.

Prasyarat

Saat Anda menggunakan AD Connector, Anda perlu mendelegasikan izin tambahan ke akun layanan. Atur daftar kontrol akses (ACL) pada akun layanan Anda untuk memberi diri Anda kemampuan untuk melakukan hal berikut.

- Tambahkan dan hapus Service Principal Name (SPN) ke dirinya sendiri.

- Buat dan perbarui otoritas sertifikasi dalam wadah berikut:

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- Buat dan perbarui objek Otoritas AuthCertificates Sertifikasi NT seperti contoh di bawah ini. Jika objek Otoritas AuthCertificates Sertifikasi NT ada, Anda harus mendelegasikan izin untuk itu. Jika objek tidak ada, Anda harus mendelegasikan kemampuan untuk membuat objek anak pada wadah Layanan Kunci Publik.

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> Jika Anda menggunakan Microsoft AD AWS Terkelola, izin tambahan akan didelegasikan secara otomatis saat Anda mengotorisasi layanan AWS Private CA Konektor untuk AD dengan direktori Anda.

Anda dapat menggunakan PowerShell skrip berikut untuk mendelegasikan izin tambahan dan membuat objek otoritas AuthCertifiates sertifikasi NT. Ganti 'myconnectoraccount' dengan nama akun layanan.

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE

# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
```

```
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGuid, 'None'
$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"

# Add ACLs allowing AD Connector service account the ability to create certification
 authorities
[System.GUID]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'certificationAuthority' }
 -Properties 'schemaIDGUID').schemaIDGUID
$CAAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
 $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
```

```
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
 @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
 -Path "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.GUID]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

Untuk mengatur AWS Private CA Konektor untuk AD

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol dihttps://console.aws.amazon.com/directoryservicev2/.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah tab Jaringan & Keamanan, di bawah AWS Private CA Konektor untuk AD, pilih Siapkan AWS Private CA Konektor untuk AD. Halaman Buat sertifikat CA Pribadi untuk Active Directory muncul. Ikuti langkah-langkah di konsol untuk membuat CA Pribadi untuk Active Directory konektor untuk mendaftar dengan CA Pribadi Anda. Untuk informasi selengkapnya, lihat Membuat konektor.
4. Setelah membuat konektor, ikuti langkah-langkah di bawah ini untuk melihat detail, termasuk status konektor dan status Private CA terkait.

Untuk melihat AWS Private CA Konektor untuk AD

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol dihttps://console.aws.amazon.com/directoryservicev2/.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Di bawah Jaringan & Keamanan, di bawah AWS Private CA Konektor untuk AD, Anda dapat melihat konektor CA Pribadi dan CA Pribadi terkait. Secara default, Anda melihat bidang berikut:
    a. AWS Private CA Connector ID — Pengidentifikasi unik untuk AWS Private CA konektor. Mengkliknya mengarah ke halaman detail AWS Private CA konektor itu.

b. AWS Private CA subjek — Informasi tentang nama yang dibedakan untuk CA. Mengkliknya mengarah ke halaman detail itu AWS Private CA.

c. Status - Berdasarkan pemeriksaan status untuk AWS Private CA Konektor dan AWS Private CA. Jika kedua pemeriksaan lulus, Active akan ditampilkan. Jika salah satu pemeriksaan gagal, 1/2 pemeriksaan gagal ditampilkan. Jika kedua pemeriksaan gagal, Gagal ditampilkan. Untuk informasi selengkapnya tentang status gagal, arahkan kursor ke hyperlink untuk mengetahui pemeriksaan mana yang gagal. Ikuti instruksi di konsol untuk memulihkan.

d. Tanggal dibuat - Hari AWS Private CA Konektor dibuat.

Untuk informasi selengkapnya, lihat Lihat detail konektor.

Memantau direktori AD Connector Anda

Anda dapat memantau direktori AD Connector Anda dengan metode berikut:

Topik

- Memahami status direktori Anda
- Konfigurasikan pemberitahuan status direktori dengan Amazon SNS

Memahami status direktori Anda

Berikut ini adalah berbagai status untuk direktori.

Aktif

Direktori beroperasi secara normal. Tidak ada masalah yang terdeteksi oleh AWS Directory Service untuk direktori Anda.

Creating

Direktori saat ini sedang dibuat. Pembuatan direktori biasanya memakan waktu antara 20 sampai 45 menit tetapi dapat bervariasi tergantung pada beban sistem.

Dihapus

Direktori telah dihapus. Semua sumber daya untuk direktori telah dirilis. Setelah direktori memasuki keadaan ini, direktori tidak dapat dipulihkan.

Deleting

Direktori saat ini sedang dihapus. Direktori akan tetap dalam keadaan ini sampai benar-benar dihapus. Setelah direktori memasuki keadaan ini, operasi hapus tidak dapat dibatalkan, dan direktori tidak dapat dipulihkan.

Failed

Direktori tidak dapat dibuat. Harap hapus direktori ini. Jika masalah ini berlanjut, hubungi PusatAWS Support.

Terganggu

Direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh. Terdapat banyak potensi alasan untuk keadaan direktori seperti ini. Ini termasuk aktivitas pemeliharaan operasional normal seperti patching atau rotasi instans EC2, hot spotting sementara oleh aplikasi pada salah satu pengendali domain Anda, atau perubahan yang Anda buat ke jaringan Anda yang secara tidak sengaja mengganggu komunikasi direktori. Untuk informasi selengkapnya, lihat salah satu dari Pemecahan Masalah AWS Microsoft AD yang Dikelola, Memecahkan masalah AD Connector, Pemecahan masalah Simple AD. Untuk masalah terkait pemeliharaan normal, AWS selesaikan masalah ini dalam waktu 40 menit. Jika setelah meninjau topik pemecahan masalah, direktori Anda dalam keadaan Terganggu lebih dari 40 menit, kami merekomendasikan Anda untuk menghubungi PusatAWS Support.

> **Important**
>
> Jangan memulihkan snapshot ketika direktori dalam keadaan Terganggu. Sangatlah jarang pemulihan snapshot diperlukan untuk mengatasi gangguan. Untuk informasi selengkapnya, lihat Snapshot atau pulihkan direktori Anda.

Tidak bisa dioperasikan

Direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.

Diminta

Permintaan untuk membuat direktori Anda sedang tertunda.

RestoreFailed

Memulihkan direktori dari snapshot gagal. Silakan coba lagi operasi pemulihan. Jika ini berlanjut, cobalah snapshot yang berbeda, atau hubungi AWS Support Pusat.

Memulihkan

Direktori saat ini sedang dipulihkan dari snapshot otomatis atau manual. Memulihkan dari snapshot biasanya memakan waktu beberapa menit, tergantung pada ukuran data direktori dalam snapshot.

Konfigurasikan pemberitahuan status direktori dengan Amazon SNS

Menggunakan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) saat status direktori Anda berubah. Anda akan diberitahu jika direktori Anda berubah dari status Aktif ke status Terganggu atau Tidak dapat dioperasikan. Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Cara kerjanya

Amazon SNS menggunakan “topik” untuk mengumpulkan dan mendistribusikan pesan. Setiap topik memiliki satu atau lebih pelanggan yang menerima pesan yang telah diterbitkan untuk topik tersebut. Dengan menggunakan langkah-langkah di bawah ini, Anda dapat menambahkan AWS Directory Service sebagai penerbit ke topik Amazon SNS. Saat AWS Directory Service mendeteksi perubahan dalam status direktori Anda, ia menerbitkan pesan ke topik tersebut, yang kemudian dikirim ke pelanggan topik tersebut.

Anda dapat mengaitkan beberapa direktori sebagai penerbit ke satu topik. Anda juga dapat menambahkan pesan status direktori ke topik yang sebelumnya Anda buat di Amazon SNS. Anda memiliki kendali terperinci atas siapa yang dapat menerbitkan dan berlangganan topik. Untuk informasi lengkap tentang Amazon SNS, lihat Apa yang Dimaksud dengan Amazon SNS?.

Untuk mengaktifkan olahpesan SNS untuk direktori Anda

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih Tindakan, dan kemudian pilih Buat notifikasi.

5. Pada halaman Buat notifikasi, pilih Pilih jenis notifikasi, lalu pilih Buat notifikasi baru. Atau, jika Anda sudah memiliki topik SNS yang ada, Anda dapat memilih Mengasosiasikan topik SNS yang ada untuk mengirim pesan status dari direktori ini ke topik tersebut.

   > **Note**
   >
   > Jika Anda memilih Buat notifikasi baru tetapi kemudian menggunakan nama topik yang sama untuk topik SNS yang sudah ada, Amazon SNS tidak membuat topik baru, tetapi hanya menambahkan informasi langganan baru ke topik yang ada.
   > Jika Anda memilih Mengasosiasikan topik SNS yang ada, Anda hanya akan dapat memilih topik SNS yang ada di Region yang sama dengan direktori.

6. Pilih Jenis penerima dan masukkan informasi kontak Penerima. Jika Anda memasukkan nomor telepon untuk SMS, gunakan angka saja. Jangan menyertakan tanda hubung, spasi, atau tanda kurung.
7. (Opsional) Berikan nama untuk topik Anda dan nama tampilan SNS. Nama tampilan adalah nama pendek hingga 10 karakter yang disertakan dalam semua pesan SMS dari topik ini. Bila menggunakan opsi SMS, nama tampilan diperlukan.

   > **Note**
   >
   > Jika Anda masuk menggunakan pengguna IAM atau peran yang hanya memiliki kebijakan DirectoryServiceFullAccessterkelola, nama topik Anda harus dimulai dengan “DirectoryMonitoring”. Jika Anda ingin menyesuaikan nama topik Anda lebih lanjut, Anda memerlukan hak istimewa tambahan untuk SNS.

8. Pilih Buat.

Jika Anda ingin menunjuk pelanggan SNS tambahan, seperti alamat email tambahan, antrian Amazon SQS AWS Lambdaatau, Anda dapat melakukan ini dari konsol Amazon SNS.

Untuk menghapus pesan status direktori dari topik

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.

4. Di bagian Pemantauan direktori, pilih nama topik SNS dalam daftar, pilih Tindakan, dan kemudian pilih Hapus.
5. Pilih Hapus.

Ini akan menghapus direktori Anda sebagai penerbit untuk topik SNS yang dipilih. Jika Anda ingin menghapus seluruh topik, Anda dapat melakukan ini dari konsol Amazon SNS.

> **Note**
>
> Sebelum menghapus topik Amazon SNS menggunakan konsol SNS, Anda harus memastikan bahwa direktori tidak mengirim pesan status untuk topik tersebut.
> Jika Anda menghapus topik Amazon SNS menggunakan konsol SNS, perubahan ini tidak akan segera tercermin dalam konsol Directory Service. Anda hanya akan diberitahu pada saat direktori menerbitkan notifikasi untuk topik yang dihapus, dalam hal ini Anda akan melihat status diperbarui pada tab Pemantauan direktori yang menunjukkan topik tidak dapat ditemukan.
> Oleh karena itu, untuk menghindari kehilangan pesan status direktori penting, sebelum menghapus topik apa pun yang menerima pesan dari AWS Directory Service, kaitkan direktori Anda dengan topik Amazon SNS yang berbeda.

Bergabunglah dengan instans EC2 ke Active Directory Anda

AD Connector adalah gateway direktori yang mana Anda dapat mengalihkan permintaan direktori ke Microsoft Active Directory on-premise Anda tanpa menyimpan informasi apa pun di cloud. Berikut informasi selengkapnya tentang bagaimana Anda dapat bergabung dengan Amazon EC2 ke domain Direktori Aktif:

- Anda dapat menggabungkan instans EC2 dengan mulus ke domain Active Directory saat instans diluncurkan. Untuk informasi selengkapnya, lihat Menggabungkan instance Windows dengan mulus ke domain Microsoft AD yang AWS Dikelola.
- Jika Anda perlu menggabungkan instans EC2 secara manual ke domain Active Directory, Anda harus meluncurkan instance di grup atau subnet yang tepat Wilayah AWS dan keamanan, lalu bergabung dengan instance tersebut ke domain Active Directory.
- Untuk dapat terhubung dari jarak jauh ke instans ini, Anda harus memiliki konektivitas IP ke instans dari jaringan di mana Anda menghubungkannya dari. Dalam kebanyakan kasus, ini mengharuskan

gateway internet dilampirkan ke VPC Amazon Anda dan instans tersebut memiliki alamat IP publik. Untuk informasi selengkapnya tentang menghubungkan ke internet menggunakan gateway internet lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.

> **Note**
>
> Setelah Anda menggabungkan instans ke Active Directory (lokal) yang dikelola sendiri, instans akan berkomunikasi langsung dengan Active Directory dan melewati AD Connector.

Topik

- Bergabunglah dengan instans Windows EC2 dengan mulus ke Active Directory Anda dengan AD Connector
- Bergabunglah dengan instans Linux EC2 dengan mulus ke Active Directory Anda dengan AD Connector

Bergabunglah dengan instans Windows EC2 dengan mulus ke Active Directory Anda dengan AD Connector

Prosedur ini menggabungkan instans Windows EC2 dengan mulus ke direktori AWS Microsoft AD Terkelola Anda.

Untuk bergabung dengan instans Windows EC2 dengan mulus

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).

7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.

   a. Untuk membuat key pair baru, pilih Create new key pair.

   b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.

   c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.

   d. Pilih create key pair.

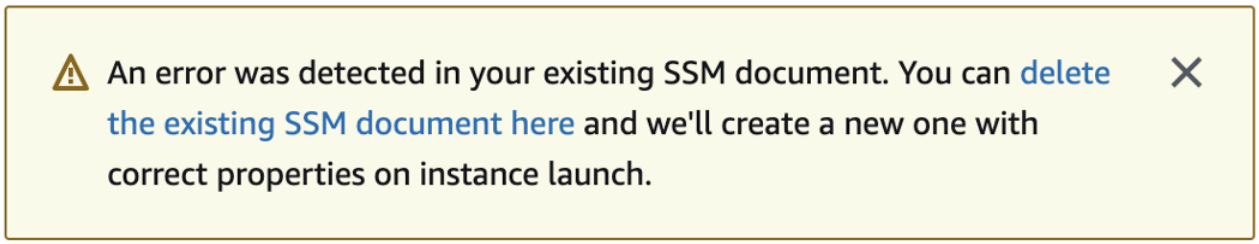
   e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

   > **Important**
   >
   > Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

    Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:
>
> 
>
>
> Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu hal berikut:
>
> - Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
> - Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola AmazonSSM ManagedInstanceCore dan AmazonSSM yang DirectoryServiceAccess dilampirkan padanya dari daftar tarik-turun profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

    1. Pilih Buat peran.
    2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.
    3. Di bawah Kasus penggunaan, pilih EC2.
    4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih kebijakan AmazonSSM dan AmazonSSM ManagedInstanceCore. DirectoryServiceAccess Untuk memfilter daftar, **`SSM`** ketik kotak pencarian. Pilih Berikutnya.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya

tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
7. Pilih Buat peran.
8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.

16. Pilih Luncurkan instans.

Bergabunglah dengan instans Linux EC2 dengan mulus ke Active Directory Anda dengan AD Connector

Prosedur ini menggabungkan instans EC2 Linux dengan mulus ke direktori AWS Microsoft AD Terkelola Anda.

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 tidak mendukung fitur penggabungan domain mulus.

Prasyarat

Sebelum Anda dapat mengatur penggabungan domain mulus ke instans EC2 Linux, Anda harus menyelesaikan prosedur di bagian ini.

Pilih akun layanan penggabungan domain mulus Anda

Anda dapat menggabungkan komputer Linux secara mulus ke domain Direktori Aktif on-premise Anda melalui AD Connector. Untuk melakukannya, Anda harus membuat akun pengguna dengan membuat izin akun komputer untuk menggabungkan komputer ke domain. Anda dapat menggunakan akun layanan AD Connector jika Anda mau. Atau Anda dapat menggunakan akun lain yang memiliki hak istimewa yang memadai untuk menggabungkan komputer ke domain. Meskipun anggota Admin Domain atau grup lain mungkin memiliki hak istimewa yang memadai untuk menggabungkan komputer ke domain, kami tidak menyarankan untuk menggunakan ini. Sebagai praktik terbaik, kami rekomendasikan Anda menggunakan akun layanan yang memiliki hak istimewa minimum yang diperlukan untuk menggabungkan komputer ke domain.

Untuk mendelegasikan akun dengan hak istimewa minimum yang diperlukan untuk bergabung dengan komputer ke domain, Anda dapat menjalankan perintah berikut PowerShell . Anda harus menjalankan perintah ini dari komputer Windows menggabungkan domain dengan Instal Alat Administrasi Direktori Aktif untuk Microsoft AD yang AWS Dikelola yang diinstal. Selain itu, Anda harus menggunakan akun yang memiliki izin untuk mengubah izin di OU komputer atau kontainer Anda. PowerShell Perintah menetapkan izin yang memungkinkan akun layanan untuk membuat objek komputer dalam wadah komputer default domain Anda. Jika Anda lebih suka menggunakan antarmuka pengguna grafis (GUI) Anda dapat menggunakan proses manual yang dijelaskan di Mendelegasikan hak istimewa ke akun layanan Anda.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
```

```
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Jika Anda lebih suka menggunakan antarmuka pengguna grafis (GUI) Anda dapat menggunakan proses manual yang dijelaskan di Mendelegasikan hak istimewa ke akun layanan Anda.

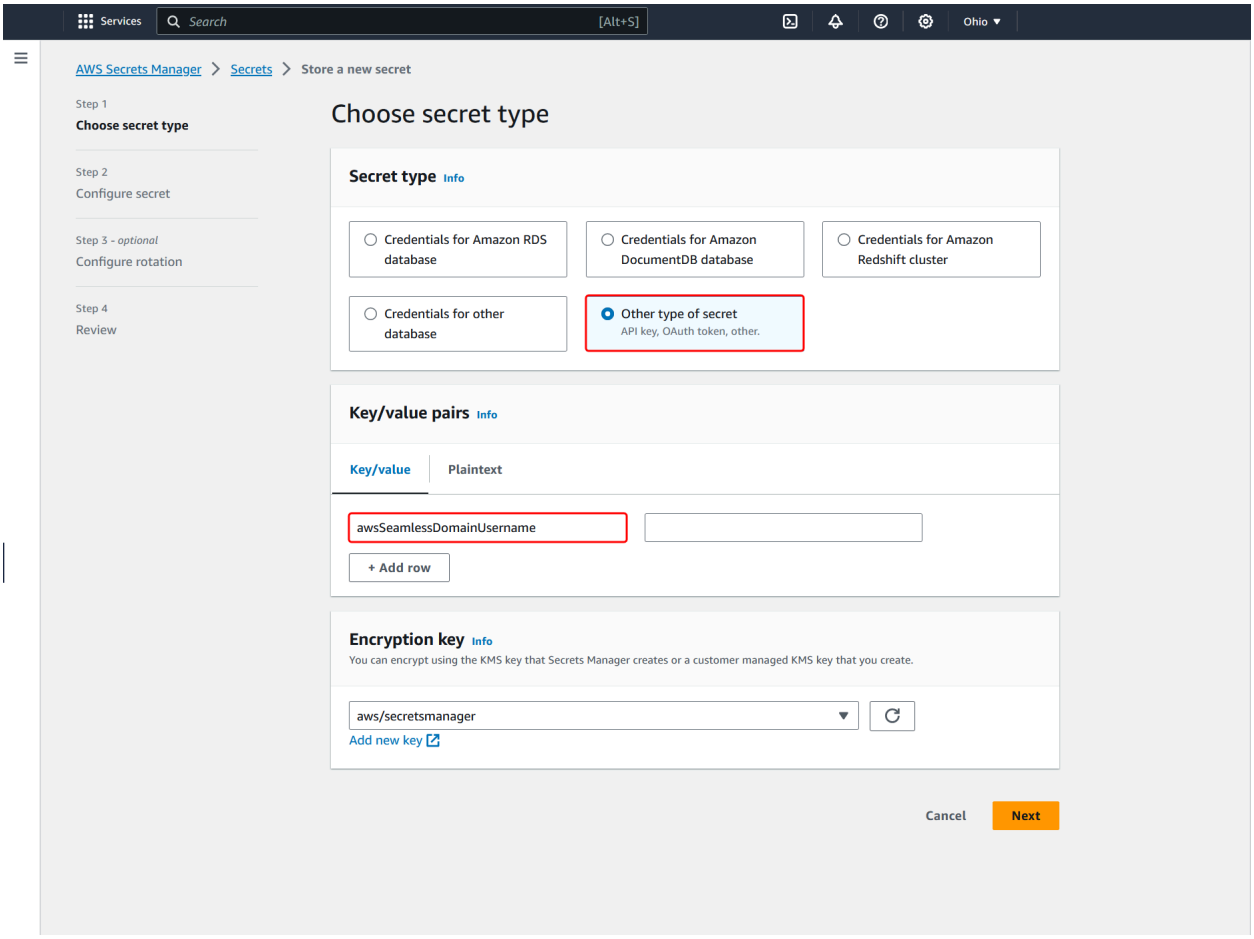
Membuat rahasia untuk menyimpan akun layanan domain

Anda dapat menggunakan AWS Secrets Manager untuk menyimpan akun layanan domain.

Untuk Membuat rahasia dan menyimpan informasi akun layanan domain

1. Masuk ke AWS Management Console dan buka AWS Secrets Manager konsol di https://console.aws.amazon.com/secretsmanager/.
2. Pilih Simpan rahasia baru.
3. Pada halaman Simpan rahasia baru, lakukan hal berikut:
   a. Di bawah Tipe rahasia, pilih Jenis rahasia lainnya.
   b. Di bawah pasangan kunci/nilai, lakukan hal berikut:
      i. Dalam kotak pertama, masukkan **`awsSeamlessDomainUsername`**. Pada baris yang sama, di kotak berikutnya, masukkan nama pengguna untuk akun layanan Anda. Misalnya, jika Anda menggunakan PowerShell perintah sebelumnya, nama akun layanan akan menjadi**`awsSeamlessDomain`**.

> **Note**
>
> Anda harus memasukkan **`awsSeamlessDomainUsername`** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.



ii. Pilih Tambahkan baris.

iii. Pada baris baru, di kotak pertama, masukkan **`awsSeamlessDomainPassword`**. Pada baris yang sama, di kotak berikutnya, masukkan kata sandi untuk akun layanan Anda.

> **Note**
>
> Anda harus memasukkan **`awsSeamlessDomainPassword`** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

iv. Di bawah kunci Enkripsi, tinggalkan nilai default`aws/secretsmanager`. AWS Secrets Manager selalu mengenkripsi rahasia ketika Anda memilih opsi ini. Anda juga dapat memilih kunci yang Anda buat.

> **Note**
>
> Ada biaya yang terkait AWS Secrets Manager, tergantung pada rahasia yang Anda gunakan. Untuk daftar harga lengkap saat ini, lihat AWS Secrets Manager Harga.
> Anda dapat menggunakan kunci AWS terkelola `aws/secretsmanager` yang dibuat Secrets Manager untuk mengenkripsi rahasia Anda secara gratis. Jika Anda membuat kunci KMS Anda sendiri untuk mengenkripsi rahasia Anda, AWS menagih Anda dengan tarif saat ini AWS KMS . Untuk informasi selengkapnya, silakan lihat Harga AWS Key Management Service.

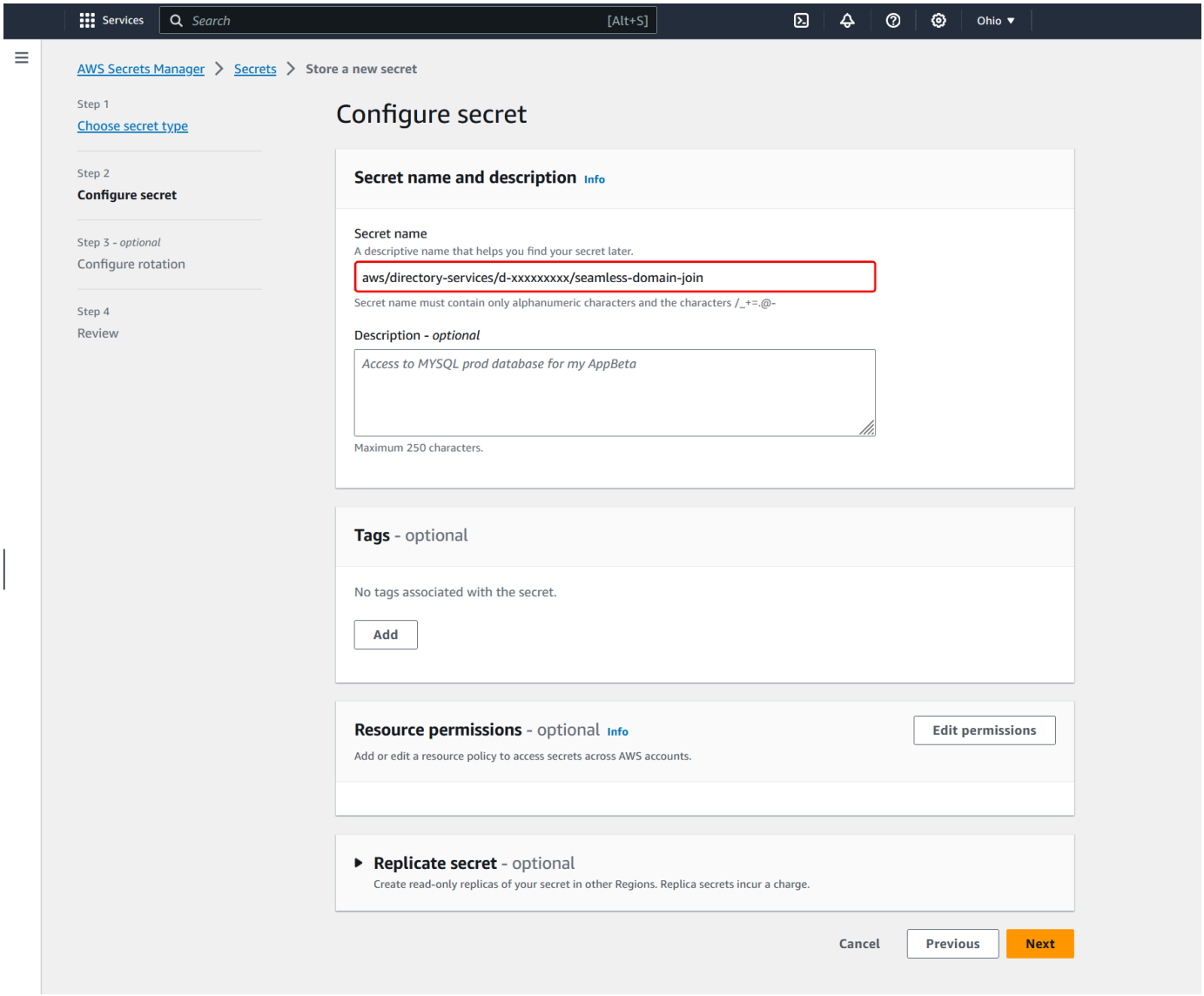
v. Pilih Berikutnya.

4. Di bawah nama Rahasia, masukkan nama rahasia yang menyertakan ID direktori Anda menggunakan format berikut, ganti *d-xxxxxxxxx* dengan ID direktori Anda:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Ini akan digunakan untuk mengambil rahasia dalam aplikasi.

> **Note**
>
> Anda harus memasukkan **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** persis seperti itu tapi ganti *d-xxxxxxxxx* dengan ID direktori Anda. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.



5. Biarkan yang lainnya diatur ke default, dan kemudian pilih Selanjutnya.
6. Di bawah Konfigurasikan rotasi otomatis, pilih Nonaktifkan rotasi otomatis, lalu pilih Selanjutnya.
7. Tinjau pengaturan, dan kemudian pilih Simpan untuk menyimpan perubahan Anda. Konsol Secrets Manager mengembalikan Anda ke daftar rahasia di akun Anda dengan rahasia baru Anda masuk di dalam daftar.
8. Pilih nama rahasia Anda yang baru dibuat dari daftar, dan perhatikan nilai ARN rahasia. Anda akan membutuhkannya di bagian selanjutnya.

Untuk membuat kebijakan dan peran IAM yang diperlukan

Gunakan langkah-langkah prasyarat berikut untuk membuat kebijakan khusus yang memungkinkan akses hanya-baca ke rahasia gabungan domain tanpa batas Secrets Manager Anda (yang Anda buat sebelumnya), dan untuk membuat peran IAM LinuxEC2 baru. DomainJoin

Membuat kebijakan membaca IAM Secrets Manager

Anda menggunakan konsol IAM untuk membuat kebijakan yang memberikan akses hanya-baca ke rahasia Secrets Manager Anda.

Untuk membuat kebijakan membaca IAM Secrets Manager

1. Masuk ke pengguna AWS Management Console sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Lalu buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, Manajemen Akses, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pilih tab JSON dan salin teks dari dokumen kebijakan JSON berikut. Kemudian tempelkan ke dalam kotak teks JSON.

> **Note**
>
> Pastikan Anda mengganti Region and Resource ARN dengan Region dan ARN sebenarnya dari rahasia yang Anda buat sebelumnya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
```

```
    ]
}
```

5. Setelah selesai, pilih Selanjutnya. Validator kebijakan melaporkan kesalahan sintaksis. Untuk informasi selengkapnya, lihat Memvalidasi kebijakan IAM.
6. Pada halaman Tinjau kebijakan, masukkan nama kebijakan, seperti **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`**. Tinjau bagian Ringkasan untuk melihat izin yang diberikan oleh kebijakan Anda. Lalu pilih Buat kebijakan untuk menyimpan perubahan Anda. Kebijakan baru muncul di daftar kebijakan terkelola dan siap dilampirkan pada identitas.

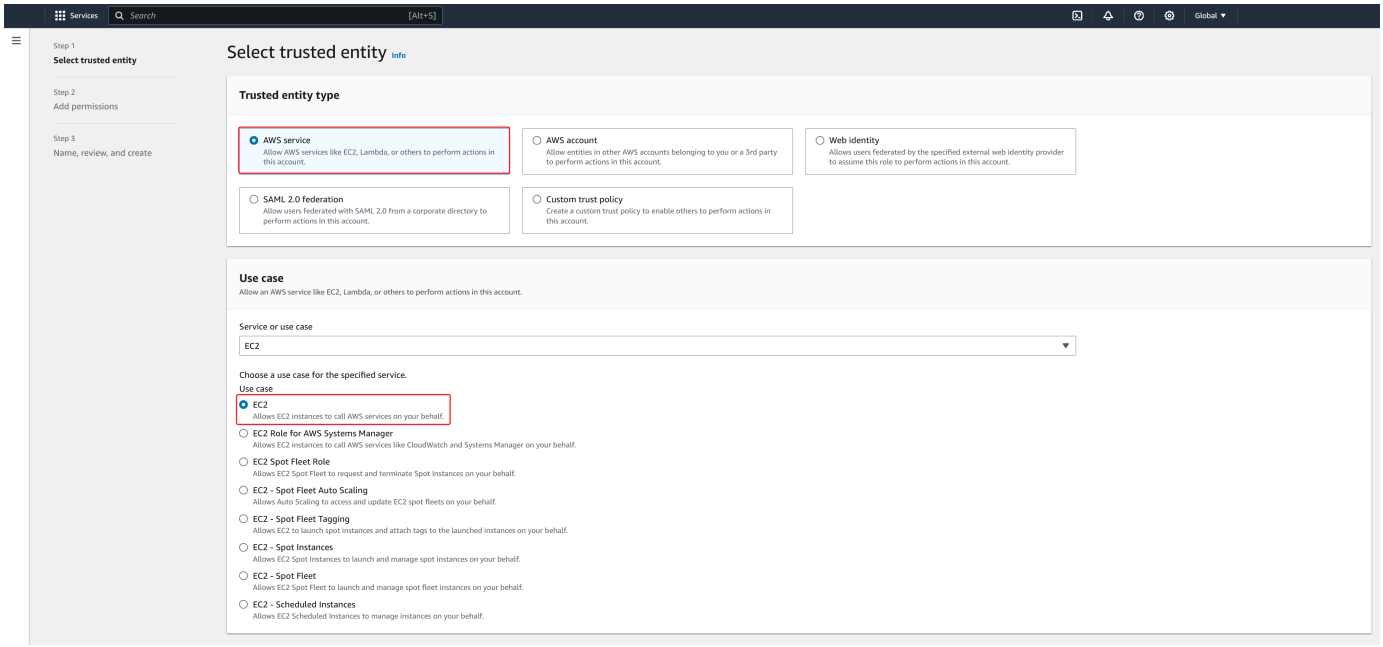
> **Note**
>
> Kami rekomendasikan Anda membuat satu kebijakan per rahasia. Melakukan hal tersebut memastikan bahwa instans hanya memiliki akses ke rahasia yang sesuai dan meminimalkan dampak jika sebuah instans dikompromikan.

Buat peran LinuXEC2 DomainJoin

Anda menggunakan konsol IAM untuk membuat peran yang akan Anda gunakan untuk penggabungan domain dengan instans EC2 Linux Anda.

Untuk membuat peran LinuXEC2 DomainJoin

1. Masuk ke pengguna AWS Management Console sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Lalu buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, di bawah Manajemen Akses, pilih Peran.
3. Di panel konten, pilih Buat peran.
4. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
5. Di bawah Kasus penggunaan, pilih EC2, lalu pilih Berikutnya.



6. Untuk Kebijakan filter, lakukan hal berikut:

   a. Masukkan **`AmazonSSMManagedInstanceCore`**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   b. Masukkan **`AmazonSSMDirectoryServiceAccess`**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   c. Masukkan **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (atau nama kebijakan yang Anda buat dalam prosedur sebelumnya). Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   d. Setelah menambahkan tiga kebijakan yang tercantum di atas, pilih Buat peran.

> **Note**
>
> AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory Service AmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

7. Masukkan nama untuk peran baru Anda, seperti **`LinuxEC2DomainJoin`** atau nama lain yang Anda inginkan di bidang Nama peran.
8. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
9. (Opsional) Pilih Tambahkan tag baru di bawah Langkah 3: Tambahkan tag untuk menambahkan tag. Pasangan nilai kunci tag digunakan untuk mengatur, melacak, atau mengontrol akses untuk peran ini.
10. Pilih Buat peran.

Bergabunglah dengan instans EC2 Linux Anda dengan mulus ke direktori AWS Microsoft AD yang Dikelola

Sekarang setelah Anda mengonfigurasi semua tugas prasyarat, Anda dapat menggunakan prosedur berikut untuk bergabung dengan instans Linux EC2 Anda dengan mulus.

Untuk bergabung dengan instans Linux Anda dengan mulus

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Dari pemilih Region di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Name and Tags, masukkan nama yang ingin Anda gunakan untuk instans Linux EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih AMI Linux yang ingin Anda luncurkan.

> **Note**
>
> AMI yang digunakan harus memiliki AWS Systems Manager (Agen SSM) versi 2.3.1644.0 atau lebih tinggi. Untuk memeriksa versi SSM Agent yang diinstal di AMI Anda dengan meluncurkan sebuah instans dari AMI tersebut, lihat Mendapatkan versi Agen SSM yang saat ini diinstal. Jika Anda perlu meningkatkan Agen SSM, lihat Menginstal dan mengkonfigurasi SSM Agent pada instans EC2 untuk Linux.
> SSM menggunakan `aws:domainJoin` plugin saat menggabungkan instance Linux ke Active Directory domain. *`Plugin mengubah nama host untuk instance Linux`*

ke format EC2AMAZ- XXXXXXX. Untuk informasi selengkapnya`aws:domainJoin`, lihat referensi plugin dokumen AWS Systems Manager perintah di Panduan AWS Systems Manager Pengguna.

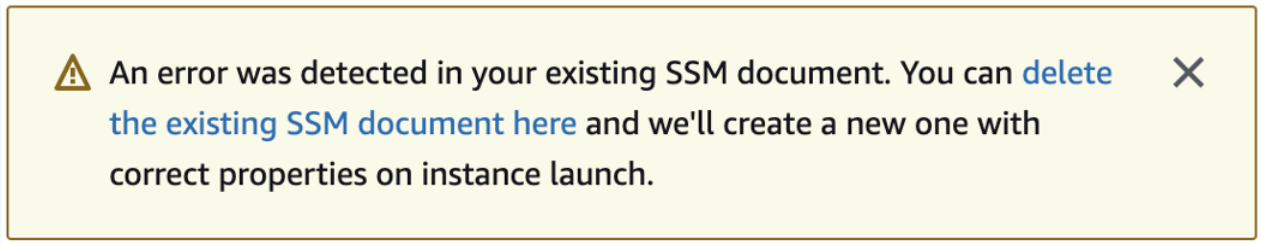
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada. Untuk membuat key pair baru, pilih Create new key pair. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk. Pilih create key pair. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

   Important

   Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.
9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

    Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:
>
> 
>
>
> Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu hal berikut:
>
> - Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
> - Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, pilih peran IAM yang sebelumnya Anda buat di bagian prasyarat Langkah 2: Buat peran LinuxEC2. DomainJoin
16. Pilih Luncurkan instans.

> **Note**
>
> Jika Anda menjalankan penggabungan domain yang mulus dengan SUSE Linux, reboot diperlukan sebelum autentikasi akan bekerja. Untuk me-reboot SUSE dari terminal Linux, ketik sudo reboot.

Memelihara direktori AD Connector

Bagian ini menjelaskan cara memelihara tugas administratif umum untuk lingkungan AD Connector Anda.

Topik

- Hapus AD Connector

- Melihat informasi direktori

Hapus AD Connector

Saat Konektor AD dihapus, direktori lokal Anda tetap utuh. Semua instans yang bergabung ke direktori juga tetap utuh dan tetap bergabung ke direktori on-premise Anda. Anda masih bisa menggunakan kredensial direktori Anda untuk masuk ke instans ini.

Untuk menghapus AD Connector

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori. Pastikan Anda berada di Wilayah AWS tempat AD Connector digunakan. Untuk informasi selengkapnya, lihat Memilih Wilayah.
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk AD Connector yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus AD Connector Anda.

   a. Pada halaman Direktori, pilih ID direktori Anda.

   b. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk AD Connector Anda.

      - Nonaktifkan AWS Management Console akses.
      - Untuk menonaktifkan Amazon WorkSpaces, Anda harus membatalkan pendaftaran layanan dari direktori di konsol. WorkSpaces Untuk informasi selengkapnya, lihat membatalkan pendaftaran dari direktori di Panduan Administrasi Amazon WorkSpaces .
      - Untuk menonaktifkan Amazon WorkDocs, Anda harus menghapus WorkDocs situs Amazon di WorkDocs konsol Amazon. Untuk informasi selengkapnya, lihat Menghapus situs di Panduan WorkDocs Administrasi Amazon.
      - Untuk menonaktifkan Amazon WorkMail, Anda harus menghapus WorkMail organisasi Amazon di WorkMail konsol Amazon. Untuk informasi selengkapnya, lihat Menghapus organisasi di Panduan WorkMail Administrator Amazon.
      - Untuk menonaktifkan Amazon FSx for Windows File Server, Anda harus menghapus sistem file Amazon FSx dari domain. Untuk informasi selengkapnya, lihat Bekerja dengan Active Directory di FSx for Windows File Server di Panduan Pengguna Amazon FSx for Windows File Server.
      - Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat Mengelola instans DB dalam domain dalam Panduan Pengguna Amazon RDS.

- Untuk menonaktifkan AWS Client VPN Layanan, Anda harus menghapus layanan direktori dari Endpoint Client VPN. Untuk informasi selengkapnya, lihat Active DirectoryOtentikasi di Panduan AWS Client VPN Administrator.
- Untuk menonaktifkan Amazon Connect, Anda harus menghapus Instans Amazon Connect. Untuk informasi selengkapnya, lihat Menghapus instans Amazon Connect dalam Panduan Administrator Amazon Connect.
- Untuk menonaktifkan Amazon QuickSight, Anda harus berhenti berlangganan dari Amazon QuickSight. Untuk informasi selengkapnya, lihat Menutup Amazon QuickSight akun Anda di Panduan QuickSight Pengguna Amazon.

> **Note**
>
> Jika Anda menggunakan AWS IAM Identity Center dan sebelumnya telah menghubungkannya ke direktori Microsoft AD AWS Terkelola yang ingin Anda hapus, Anda harus terlebih dahulu mengubah sumber identitas sebelum dapat menghapusnya. Untuk informasi selengkapnya, lihat Mengubah sumber identitas Anda di Panduan Pengguna Pusat Identitas IAM.

3. Di panel navigasi, pilih Direktori.
4. Pilih hanya AD Connector yang akan dihapus dan klik Delete. Dibutuhkan beberapa menit agar AD Connector dihapus. Ketika AD Connector telah dihapus, itu dihapus dari daftar direktori Anda.

Melihat informasi direktori

Anda dapat melihat informasi detail tentang direktori.

Untuk melihat informasi direktori terperinci.

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori.
2. Klik tautan ID direktori untuk direktori Anda. Informasi tentang direktori ditampilkan dalam halaman Detail direktori.

Untuk informasi selengkapnya tentang bidang Status, lihat Memahami status direktori Anda.

Aktifkan akses ke AWS aplikasi dan layanan

Pengguna dapat mengotorisasi AD Connector untuk memberikan AWS aplikasi dan layanan, seperti Amazon WorkSpaces, akses ke aplikasi AndaActive Directory. AWS Aplikasi dan layanan berikut dapat diaktifkan atau dinonaktifkan untuk bekerja dengan AD Connector.

AWS aplikasi/layanan	Informasi selengkapnya…
Amazon Chime	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Chime.
Amazon Connect	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Connect.
Amazon WorkDocs	Untuk informasi selengkapnya, lihat Panduan WorkDocs Administrasi Amazon.
Amazon WorkMail	Untuk informasi selengkapnya, lihat Panduan WorkMail Administrator Amazon.
Amazon WorkSpaces	Anda dapat membuat Simple AD, AWS Managed Microsoft AD, atau AD Connector langsung dari WorkSpaces. Cukup luncurkan Pengaturan Advanced saat membuat Workspace Anda. Untuk informasi selengkapnya, lihat Panduan WorkSpaces Administrasi Amazon.
AWS Client VPN	Untuk informasi selengkapnya, silakan lihat Panduan PenggunaAWS Client VPN.
AWS IAM Identity Center	Untuk informasi selengkapnya, lihat Panduan PenggunaAWS IAM Identity Center.
AWS Management Console	Untuk informasi selengkapnya, lihat Mengaktifkan akses ke AWS Management Console dengan kredensial AD.

AWS aplikasi/layanan	Informasi selengkapnya…
AWS Transfer Family	Untuk informasi selengkapnya, silakan lihat Panduan PenggunaAWS Transfer Family.

Setelah diaktifkan, Anda mengelola akses ke direktori Anda di konsol dari aplikasi atau layanan yang ingin Anda berikan akses ke direktori Anda. Untuk menemukan tautan AWS aplikasi dan layanan yang dijelaskan di atas di AWS Directory Service konsol, lakukan langkah-langkah berikut.

Untuk menampilkan aplikasi dan layanan untuk direktori

1. Pada panel navigasi konsolAWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Tinjau daftar di bawah bagian aplikasi & layananAWS .

Untuk informasi selengkapnya tentang cara mengotorisasi atau membatalkan otorisasi AWS aplikasi dan layanan yang digunakan AWS Directory Service, lihat. Otorisasi untuk AWS aplikasi dan layanan menggunakan AWS Directory Service

Memperbarui alamat DNS untuk AD Connector Anda

Gunakan langkah-langkah berikut untuk memperbarui alamat DNS yang ditunjuk oleh AD Connector Anda.

> **Note**
>
> Jika Anda memiliki pembaruan yang sedang berlangsung, Anda harus menunggu sampai selesai sebelum mengirimkan pembaruan lain.
> Jika Anda menggunakan WorkSpaces AD Connector, pastikan alamat DNS Anda WorkSpace juga diperbarui. Untuk informasi selengkapnya, lihat Memperbarui server DNS untuk WorkSpaces.

Untuk memperbarui pengaturan DNS Anda untuk AD Connector

1. Di panel navigasi AWS Directory Servicekonsol, di bawah Active Directory, pilih Direktori.

2. Pilih tautan ID direktori untuk direktori Anda.
3. Pada halaman Detail direktori, pilih tab Jaringan & Keamanan.
4. Gulir ke bawah ke bagian Pengaturan DNS yang ada dan pilih Perbarui.
5. Di dialog Perbarui alamat DNS yang ada, ketik alamat IP DNS yang diperbarui, lalu pilihPerbarui.

Untuk informasi selengkapnya tentang pemecahan masalah AD Connector, lihat Memecahkan Masalah AD Connector.

Praktik terbaik untuk AD Connector

Berikut adalah beberapa saran dan panduan yang harus Anda pertimbangkan untuk menghindari masalah dan mendapatkan hasil maksimal dari AD Connector.

Menyiapkan: Prasyarat

Pertimbangkan panduan ini sebelum membuat direktori Anda.

Verifikasikan Anda memiliki jenis direktori yang tepat

AWS Directory Service menyediakan berbagai cara untuk digunakan dengan AWS layanan lain. Anda dapat memilih directory service dengan fitur yang Anda butuhkan dengan biaya yang sesuai dengan anggaran Anda:

- AWS Directory Service untuk Microsoft Active Directory adalah pengelola kaya fitur yang dihosting di cloud. AWS AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memiliki lebih dari 5.000 pengguna dan memerlukan hubungan kepercayaan yang disiapkan antara direktori yang AWS dihosting dan direktori lokal Anda.
- AD Connector hanya menghubungkan lokal Active Directory Anda yang sudah ada. AWS AD Connector adalah pilihan terbaik Anda saat Anda ingin menggunakan direktori on-premise Anda yang sudah ada dengan layanan AWS .
- Simple AD adalah direktori berskala rendah dan berbiaya rendah dengan kompatibilitas dasarActive Directory. Ini mendukung 5.000 atau lebih sedikit pengguna, aplikasi yang kompatibel dengan Samba 4, dan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Untuk perbandingan AWS Directory Service opsi yang lebih rinci, lihatMana yang harus dipilih.

Pastikan VPC dan instans Anda dikonfigurasi dengan benar

Untuk terhubung ke, mengelola, dan menggunakan direktori Anda, Anda harus mengkonfigurasi VPC yang terkait direktori dengan benar. Lihat AWS Prasyarat Microsoft AD yang dikelola, Prasyarat AD Connector, atau Prasyarat Simple AD untuk informasi tentang persyaratan keamanan dan jaringan VPC.

Jika Anda menambahkan instans ke domain Anda, pastikan bahwa Anda memiliki konektivitas dan akses jarak jauh ke instans Anda seperti yang dijelaskan di Bergabunglah dengan instans Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola.

Ketahui batasan Anda

Pelajari tentang berbagai batasan untuk jenis direktori spesifik Anda. Penyimpanan yang tersedia dan ukuran agregat objek Anda adalah satu-satunya keterbatasan terkait jumlah objek yang dapat Anda simpan dalam direktori Anda. Lihat Kuota Microsoft AD yang Dikelola AWS, Kuota AD Connector, atau Kuota Simple AD untuk detail tentang direktori pilihan Anda.

Memahami konfigurasi dan penggunaan grup AWS keamanan direktori Anda

AWS membuat grup keamanan dan melampirkannya ke antarmuka jaringan elastis direktori Anda yang dapat diakses dari dalam VPC peered atau diubah ukurannya. AWS mengkonfigurasi grup keamanan untuk memblokir lalu lintas yang tidak perlu ke direktori dan memungkinkan lalu lintas yang diperlukan.

Memodifikasi grup keamanan direktori

Jika Anda ingin mengubah keamanan grup keamanan direktori Anda, Anda dapat melakukannya. Hanya buat perubahan tersebut jika Anda sepenuhnya memahami cara kerja filter grup keamanan. Untuk informasi selengkapnya, lihat Grup Keamanan Amazon EC2 untuk instans Linux di Panduan Pengguna Amazon EC2. Perubahan yang tidak tepat dapat mengakibatkan hilangnya komunikasi ke komputer dan instance yang dituju. AWS merekomendasikan agar Anda tidak mencoba membuka port tambahan ke direktori Anda karena ini mengurangi keamanan direktori Anda. Harap tinjau dengan seksama Model Tanggung Jawab Bersama AWS.

> **Warning**
>
> Secara teknis Anda dapat mengasosiasikan grup keamanan direktori dengan instans EC2 lain yang Anda buat. Namun, AWS merekomendasikan untuk tidak melakukan praktik ini.

AWS mungkin memiliki alasan untuk memodifikasi grup keamanan tanpa pemberitahuan untuk mengatasi kebutuhan fungsional atau keamanan direktori terkelola. Perubahan tersebut mempengaruhi setiap instans yang Anda asosiasikan dengan grup keamanan direktori dan dapat mengganggu operasi instans terkait. Selain itu, mengaitkan grup keamanan direktori dengan instans EC2 Anda dapat menciptakan risiko keamanan potensial untuk instans EC2 Anda.

Mengkonfigurasi situs dan subnet on-premise dengan benar saat menggunakan AD Connector

Jika jaringan on-premise Anda memiliki situs Direktori Aktif yang ditetapkan, Anda harus memastikan subnet di VPC tempat AD Connector Anda berada didefinisikan di situs Direktori Aktif, dan bahwa tidak ada konflik antara subnet di VPC dan subnet di situs Anda yang lainnya.

Untuk menemukan pengendali domain, AD Connector menggunakan situs Direktori Aktif yang rentang alamat IP subnet nya dekat dengan yang ada di VPC yang berisi AD Connector. Jika Anda memiliki situs yang subnetnya memiliki rentang alamat IP yang sama seperti yang ada di VPC Anda, AD Connector akan menemukan pengendali domain di situs tersebut, yang mungkin tidak secara fisik dekat dengan Region Anda.

Memahami batasan nama pengguna untuk AWS aplikasi

AWS Directory Service memberikan dukungan untuk sebagian besar format karakter yang dapat digunakan dalam pembangunan nama pengguna. Namun, ada batasan karakter yang diberlakukan pada nama pengguna yang akan digunakan untuk masuk ke AWS aplikasi, seperti, Amazon, WorkSpaces WorkDocs Amazon WorkMail, atau Amazon. QuickSight Pembatasan ini mengharuskan karakter berikut tidak digunakan:

- Spasi
- Karakter multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

Note

Simbol @ diperbolehkan selama itu mendahului akhiran UPN.

Memprogram aplikasi Anda

Sebelum memprogram aplikasi Anda, pertimbangkan hal berikut:

Muat tes sebelum diluncurkan ke produksi

Pastikan untuk melakukan pengujian laboratorium dengan aplikasi dan permintaan yang mewakili beban kerja produksi Anda untuk mengkonfirmasi bahwa direktori meningkatkan skala ke beban aplikasi Anda. Jika Anda memerlukan kapasitas tambahan, sebarkan beban Anda di beberapa direktori AD Connector.

Menggunakan direktori Anda

Berikut adalah beberapa saran yang perlu diingat saat menggunakan direktori Anda.

Rotasi kredensial Admin secara teratur

Ubah kata sandi Admin akun layanan AD Connector Anda secara teratur, dan pastikan kata sandi konsisten dengan kebijakan kata sandi Direktori Aktif Anda yang sudah ada. Untuk petunjuk tentang cara mengubah kata sandi akun layanan, lihat Memperbarui kredensial akun layanan AD Connector Anda di AWS Directory Service.

Gunakan AD Connector unik untuk setiap domain

AD Connector dan domain AD on-premise Anda memiliki hubungan 1-banding-1. Artinya, untuk setiap domain on-premise, termasuk domain anak di hutan AD yang ingin Anda autentikasi, Anda harus membuat AD Connector yang unik. Setiap AD Connector yang Anda buat harus menggunakan akun layanan yang berbeda, meskipun terhubung ke direktori yang sama.

Periksa kompatibilitas

Saat menggunakan AD Connector, Anda harus memastikan bahwa direktori lokal Anda dan tetap kompatibel dengan AWS Directory Service s. Untuk informasi selengkapnya tentang tanggung jawab Anda, silakan lihat model tanggung jawab bersama kami.

Kuota AD Connector

Berikut ini adalah Kuota default untuk AD Connector. Kecuali dinyatakan lain, masing-masing kuota adalah per Region.

Kuota AD Connector

Resource	Kuota default
Direktori AD Connector	10
Jumlah maksimum dari sertifikat otoritas sertifikasi (CA) terdaftar per direktori	5

Kebijakan kompatibilitas aplikasi untuk AD Connector

Sebagai alternatif untuk AWS Directory Service for Microsoft Active Directory (AWS Microsoft AD yang dikelola), AD Connector adalah proksi Direktori Aktif untuk layanan dan aplikasi buatan AWS saja. Anda mengkonfigurasi proksi untuk menggunakan domain Direktori Aktif yang ditentukan. Bila aplikasi harus mencari pengguna atau grup di Direktori Aktif, AD Connector akan memproksikan permintaan ke direktori. Demikian pula ketika pengguna masuk ke aplikasi, AD Connector memproksikan permintaan autentikasi ke direktori. Tidak ada aplikasi pihak ketiga yang bekerja dengan AD Connector.

Berikut ini adalah daftar aplikasi dan layanan AWS yang kompatibel:

- Amazon Chime - Untuk instruksi detail, lihat Menghubungkan ke Direktori Aktif Anda.
- Amazon Connect - Untuk informasi selengkapnya, lihat Cara kerja Amazon Connect.
- Amazon EC2 untuk Windows atau Linux — Anda dapat menggunakan fitur gabungan domain Active Directory yang mulus dari Amazon EC2 Windows atau Linux untuk menggabungkan instans Anda ke Active Directory yang dikelola sendiri (lokal). Setelah bergabung, instans berkomunikasi langsung dengan Direktori Aktif Anda dan melewati AD Connector. Untuk informasi selengkapnya, lihat Bergabunglah dengan instans EC2 ke Active Directory Anda.
- AWS Management Console — Anda dapat menggunakan AD Connector untuk mengautentikasi pengguna AWS Management Console dengan kredensial Direktori Aktif mereka tanpa menyiapkan infrastruktur SAML. Untuk informasi selengkapnya, lihat Mengaktifkan akses ke AWS Management Console dengan kredensial AD.
- Amazon QuickSight - Untuk informasi selengkapnya, lihat Mengelola akun pengguna di Amazon QuickSight Enterprise Edition.
- AWS IAM Identity Center- Untuk petunjuk terperinci, lihat Connect IAM Identity Center ke Active Directory lokal.

- AWS Transfer Family - Untuk instruksi detail, lihat Bekerja dengan AWS Directory Service for Microsoft Active Directory.
- AWS Client VPN - Untuk instruksi detail, lihat Autentikasi dan otorisasi klien.
- Amazon WorkDocs - Untuk petunjuk mendetail, lihat Menyambungkan ke direktori lokal Anda dengan AD Connector.
- Amazon WorkMail - Untuk petunjuk terperinci, lihat Mengintegrasikan Amazon WorkMail dengan direktori yang ada (penyiapan standar).
- WorkSpaces - Untuk petunjuk terperinci, lihat Meluncurkan WorkSpace menggunakan AD Connector.

> **Note**
>
> Amazon RDS hanya kompatibel dengan Microsoft AD yang dikelola AWS, dan tidak kompatibel dengan AD Connector. Untuk informasi selengkapnya, lihat bagian AD Microsoft AWS Terkelola di halaman AWS Directory ServiceFAQ.

Memecahkan masalah AD Connector

Berikut ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat membuat atau menggunakan AD Connector.

Topik

Masalah pembuatan

Berikut ini adalah masalah pembuatan yang umum untuk AD Connector

- Saya menerima kesalahan “Masalah konektivitas terdeteksi” ketika saya mencoba membuat AD Connector

Saya menerima kesalahan “AZ Dibatasi” saat saya membuat direktori

Beberapa AWS akun yang dibuat sebelum 2012 mungkin memiliki akses ke Availability Zones di Wilayah AS Timur (Virginia N.), AS Barat (California N.), atau Asia Pasifik (Tokyo) yang tidak mendukung AWS Directory Service direktori. Jika Anda menerima kesalahan seperti ini saat membuatActive Directory, pilih subnet di Availability Zone yang berbeda dan coba buat direktori lagi.

Saya menerima kesalahan “Masalah konektivitas terdeteksi” ketika saya mencoba membuat AD Connector

Jika Anda menerima kesalahan “Masalah konektivitas terdeteksi” saat mencoba membuat Konektor AD, kesalahan mungkin karena ketersediaan port atau kompleksitas kata sandi AD Connector. Anda dapat menguji koneksi Konektor AD untuk melihat apakah port berikut tersedia:

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Untuk menguji koneksi Anda, lihatUji AD Connector Anda. Tes koneksi harus dilakukan pada instance yang digabungkan ke kedua subnet yang terkait dengan alamat IP Konektor AD.

Jika tes koneksi berhasil dan instance bergabung dengan domain, periksa kata sandi Konektor AD Anda. AD Connector harus memenuhi persyaratan kompleksitas AWS kata sandi. Untuk informasi selengkapnya, lihat Akun layanan diPrasyarat AD Connector.

Jika AD Connector Anda tidak memenuhi persyaratan ini, buat ulang AD Connector Anda dengan kata sandi yang sesuai dengan persyaratan ini.

Masalah konektivitas

Berikut ini adalah masalah konektivitas umum untuk AD Connector

- Saya menerima error “Masalah koneksi terdeteksi” ketika mencoba menghubungkan ke direktori on-premise saya

- Saya menerima error “DNS tidak tersedia” ketika mencoba menghubungkan ke direktori on-premise saya
- Saya menerima error “catatan SRV” ketika mencoba menghubungkan ke direktori on-premise saya

Saya menerima error “Masalah koneksi terdeteksi” ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan error yang serupa dengan yang berikut ini saat menghubungkan ke direktori on-premise Anda:

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
 Kerberos/authentication unavailable (TCP port 88) for IP: <IP address> Please ensure
 that the listed ports are available and retry the operation.
```

AD Connector harus dapat berkomunikasi dengan pengendali domain on-premise Anda melalui TCP dan UDP melewati port-port berikut. Verifikasi bahwa grup keamanan dan firewall on-premise mengizinkan komunikasi TCP dan UDP melewati port-port ini. Untuk informasi selengkapnya, lihat Prasyarat AD Connector.

- 88 (Kerberos)
- 389 (LDAP)

Anda mungkin memerlukan port TCP/UDP tambahan tergantung pada kebutuhan Anda. Lihat daftar berikut untuk beberapa port ini. Untuk informasi selengkapnya tentang port yang digunakanActive Directory, lihat Cara mengonfigurasi firewall untuk Active Directory domain dan trust dalam Microsoft dokumentasi.

- 135 (Pemetaan Titik Akhir RPC)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

Saya menerima error “DNS tidak tersedia” ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan error yang serupa dengan yang berikut ini saat menghubungkan ke direktori on-premise Anda:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector harus dapat berkomunikasi dengan server DNS on-premise Anda melalui TCP dan UDP melewati port 53. Verifikasi bahwa grup keamanan dan firewall on-premise mengizinkan komunikasi TCP dan UDP melewati port ini. Untuk informasi selengkapnya, lihat Prasyarat AD Connector.

Saya menerima error “catatan SRV” ketika mencoba menghubungkan ke direktori on-premise saya

Anda menerima pesan error yang serupa dengan satu atau beberapa berikut ini saat menghubungkan ke direktori on-premise Anda:

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos
 does not exist for IP: <DNS IP address>
```

AD Connector perlu memperoleh catatan SRV `_ldap._tcp.<DnsDomainName>` dan `_kerberos._tcp.<DnsDomainName>` saat menghubungkan ke direktori Anda. Anda akan mendapatkan error ini jika layanan tidak dapat memperoleh catatan ini dari server DNS yang Anda tentukan saat menghubungkan ke direktori Anda. Untuk informasi selengkapnya mengenai catatan SRV ini, lihat SRV record requirements.

Masalah otentikasi

Berikut adalah beberapa masalah otentikasi umum dengan AD Connector:

- Saya menerima kesalahan '“Validasi Sertifikat gagal” ketika saya mencoba masuk Amazon WorkSpaces dengan kartu pintar
- Saya menerima error “Kredensial Tidak Valid” saat akun layanan yang digunakan oleh AD Connector mencoba untuk mengautentikasi
- Saya menerima kesalahan “Tidak Dapat Mengautentikasi” saat menggunakan AWS aplikasi untuk mencari pengguna atau grup

- Saya menerima kesalahan tentang kredensyal direktori saya ketika saya mencoba memperbarui akun layanan AD Connector
- Beberapa pengguna saya tidak dapat mengautentikasi dengan direktori saya

Saya menerima kesalahan '"Validasi Sertifikat gagal" ketika saya mencoba masuk Amazon WorkSpaces dengan kartu pintar

Anda menerima pesan galat yang mirip dengan berikut ini ketika Anda mencoba masuk WorkSpaces dengan kartu pintar:

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

Kesalahan terjadi jika sertifikat kartu pintar tidak disimpan dengan benar pada klien yang menggunakan sertifikat. Untuk informasi selengkapnya tentang AD Connector dan persyaratan kartu pintar, lihatPrasyarat.

Gunakan prosedur berikut untuk memecahkan masalah kemampuan kartu pintar untuk menyimpan sertifikat di toko sertifikat pengguna:

1. Pada perangkat yang mengalami kesulitan mengakses sertifikat, akses Microsoft Management Console (MMC).

   > **Important**
   >
   > Sebelum bergerak maju, buat salinan sertifikat kartu pintar.

2. Arahkan ke toko sertifikat di MMC. Hapus sertifikat kartu pintar pengguna dari toko sertifikat. Untuk informasi selengkapnya tentang melihat penyimpanan sertifikat di MMC, lihat Cara: Melihat sertifikat dengan snap-in MMC dalam dokumentasi. Microsoft
3. Lepaskan kartu pintar.
4. Masukkan kembali kartu pintar sehingga dapat mengisi kembali sertifikat kartu pintar di toko sertifikat pengguna.

> **Warning**
>
> Jika kartu pintar tidak mengisi kembali sertifikat ke toko pengguna maka tidak dapat digunakan untuk otentikasi kartu WorkSpaces pintar.

Akun Layanan Konektor AD harus memiliki yang berikut:

- `my/spn`ditambahkan ke Nama Prinsip Layanan
- Delegasikan untuk layanan LDAP

Setelah sertifikat diisi kembali pada kartu pintar, pengontrol domain on-premise harus diperiksa untuk menentukan apakah mereka diblokir dari pemetaan Nama Utama Pengguna (UPN) untuk Nama Alternatif Subjek. Untuk informasi selengkapnya tentang perubahan ini, lihat Cara menonaktifkan Nama Alternatif Subjek untuk pemetaan UPN dalam Microsoft dokumentasi.

Gunakan prosedur berikut untuk memeriksa kunci registri pengontrol domain Anda:

1. Di Editor Registri, arahkan ke kunci sarang berikut

   HKEY_LOCAL_MACHINE\ SISTEM\\ Layanan\ Kdc\ CurrentControlSet UseSubjectAltName
2. Pilih UseSubjectAltName. Pastikan nilainya disetel ke 0.

> **Note**
>
> Jika kunci registri diatur pada Pengontrol Domain on-premise maka AD Connector tidak akan dapat menemukan pengguna Active Directory dan menghasilkan pesan kesalahan di atas.

Sertifikat Otoritas Sertifikat (CA) harus diunggah ke sertifikat kartu pintar AD Connector. Sertifikat harus berisi informasi OCSP. Berikut daftar persyaratan tambahan untuk CA:

- Sertifikat harus berada di Otoritas Root Tepercaya dari Pengontrol Domain, Server Otoritas Sertifikat, dan WorkSpaces.
- Sertifikat Offline dan Root CA tidak akan berisi informasi OSCP. Sertifikat ini berisi informasi tentang pencabutan mereka.

- Jika Anda menggunakan sertifikat CA pihak ketiga untuk otentikasi kartu pintar, maka CA dan sertifikat perantara harus dipublikasikan ke toko Active Directory NTAuth. Mereka harus diinstal di otoritas root tepercaya untuk semua pengontrol domain, server otoritas sertifikat, dan WorkSpaces.
  - Anda dapat menggunakan perintah follow untuk menerbitkan sertifikat ke toko Active Directory NTAuth:

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

Untuk informasi selengkapnya tentang menerbitkan sertifikat ke toko NTAuth, lihat Mengimpor sertifikat CA yang diterbitkan ke toko Enterprise NTAuth di Access Amazon WorkSpaces dengan Panduan Instalasi Kartu Akses Umum.

Anda dapat memeriksa untuk melihat apakah sertifikat pengguna atau sertifikat rantai CA diverifikasi oleh OCSP dengan mengikuti prosedur ini:

1. Ekspor sertifikat kartu pintar ke lokasi di mesin lokal seperti drive C:.
2. Buka prompt Baris Perintah dan arahkan ke lokasi penyimpanan sertifikat kartu pintar yang diekspor.
3. Masukkan perintah berikut:

```
certutil -URL Certficate_name.cer
```

4. Jendela pop-up akan muncul mengikuti perintah. Pilih opsi OCSP di sudut kanan dan pilih Ambil. Status harus kembali seperti yang diverifikasi.

Untuk informasi lebih lanjut tentang perintah certutil, lihat certutil dalam dokumentasi Microsoft

Saya menerima error “Kredensial Tidak Valid” saat akun layanan yang digunakan oleh AD Connector mencoba untuk mengautentikasi

Hal ini dapat terjadi jika hard drive pada pengendali domain Anda kehabisan ruang. Pastikan bahwa hard drive pengendali domain Anda tidak penuh.

Saya menerima kesalahan “Tidak Dapat Mengautentikasi” saat menggunakan AWS aplikasi untuk mencari pengguna atau grup

Anda mungkin mengalami kesalahan saat mencari pengguna saat menggunakan AWS aplikasi, seperti WorkSpaces atau Amazon QuickSight, bahkan saat status AD Connector aktif. Kredensial yang kedaluwarsa dapat mencegah AD Connector menyelesaikan kueri pada objek di Direktori Aktif Anda. Perbarui kata sandi untuk akun layanan menggunakan langkah-langkah yang dipesan yang disediakan diGabungan domain yang mulus untuk instans Amazon EC2 berhenti berfungsi.

Saya menerima kesalahan tentang kredensyal direktori saya ketika saya mencoba memperbarui akun layanan AD Connector

Anda menerima pesan galat yang mirip dengan satu atau beberapa hal berikut saat mencoba memperbarui akun layanan AD Connector:

```
Message:An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials.
```

```
An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials
following Update your AD Connector Service Account Credentials
```

```
Message:
An Error Has Occurred
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

Mungkin ada masalah dengan sinkronisasi waktu dan Kerberos. AD Connector mengirimkan permintaan otentikasi Kerberos ke. Active Directory Permintaan ini sensitif terhadap waktu dan jika permintaan ditunda, mereka akan gagal. Untuk mengatasi masalah ini, lihat Rekomendasi - Mengonfigurasi Root PDC dengan Sumber Waktu Otoritatif dan Hindari Kemiringan Waktu Luas dalam dokumentasi. Microsoft Untuk informasi lebih lanjut tentang layanan waktu dan sinkronisasi, lihat di bawah ini:

- Bagaimana Layanan Windows Waktu Bekerja
- Toleransi maksimum untuk sinkronisasi jam komputer
- WindowsAlat dan pengaturan layanan waktu

Beberapa pengguna saya tidak dapat mengautentikasi dengan direktori saya

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, tetapi tidak boleh diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka Preauthentication on. Microsoft TechNet

Masalah pemeliharaan

Berikut ini adalah masalah perawatan umum untuk AD Connector

- Direktori saya terjebak dalam status “Diminta”
- Gabungan domain yang mulus untuk instans Amazon EC2 berhenti berfungsi

Direktori saya terjebak dalam status “Diminta”

Jika Anda memiliki direktori yang telah berada dalam status “Diminta” selama lebih dari lima menit, coba hapus direktori dan buat ulang. Jika masalah ini berlanjut, hubungi AWS Support.

Gabungan domain yang mulus untuk instans Amazon EC2 berhenti berfungsi

Jika penggabungan domain yang mulus untuk instans EC2 bekerja dan kemudian berhenti saat AD Connector aktif, kredensial untuk akun layanan AD Connector Anda mungkin telah kedaluwarsa. Kredensyal kedaluwarsa dapat mencegah AD Connector membuat objek komputer di file Anda. Active Directory

Untuk mengatasi masalah ini, perbarui kata sandi akun layanan dalam urutan berikut sehingga kata sandi cocok:

1. Perbarui kata sandi untuk akun layanan di akun AndaActive Directory.
2. Perbarui kata sandi untuk akun layanan di AD Connector Anda di AWS Directory Service. Untuk informasi selengkapnya, lihat Memperbarui kredensial akun layanan AD Connector Anda di AWS Directory Service.

> **Important**
>
> Memperbarui kata sandi hanya di AWS Directory Service tidak mendorong perubahan kata sandi ke tempat Anda yang ada Active Directory sehingga penting untuk melakukannya dalam urutan yang ditunjukkan pada prosedur sebelumnya.

Saya tidak dapat menghapus AD Connector

Jika AD Connector beralih ke status tidak dapat dioperasikan, Anda tidak lagi memiliki akses ke pengontrol domain. Kami memblokir penghapusan AD Connector ketika masih ada aplikasi yang terhubung dengannya karena salah satu aplikasi tersebut mungkin masih menggunakan direktori. Untuk daftar aplikasi yang perlu Anda nonaktifkan untuk menghapus AD Connector Anda lihatHapus AD Connector. Jika Anda masih tidak dapat menghapus AD Connector, Anda dapat meminta bantuan melalui AWS Support.

Simple AD

Simple AD adalah direktori terkelola mandiri yang didukung oleh Samba 4 Active Directory Compatible Server. Ini tersedia dalam dua ukuran.

- Kecil - Mendukung hingga 500 pengguna (sekitar 2.000 objek termasuk pengguna, grup, dan komputer).
- Large - Mendukung hingga 5.000 pengguna (sekitar 20.000 objek termasuk pengguna, grup, dan komputer).

Simple AD menyediakan subset dari fitur yang ditawarkan oleh Microsoft AD yang Dikelola AWS, termasuk kemampuan untuk mengelola akun pengguna dan keanggotaan grup, membuat dan menerapkan kebijakan grup, terhubung dengan aman ke instans Amazon EC2, dan menyediakan sign-on tunggal (SSO) berbasis Kerberos. Namun, perhatikan bahwa Simple AD tidak mendukung fitur seperti otentikasi multi-faktor (MFA), hubungan kepercayaan dengan domain lain, Pusat Administrasi Direktori Aktif, PowerShell dukungan, tempat daur ulang Direktori Aktif, akun layanan terkelola grup, dan ekstensi skema untuk aplikasi POSIX dan Microsoft.

Simple AD menawarkan banyak keuntungan:

- Simple AD membuat lebih mudah untuk mengelola instans Amazon EC2 yang menjalankan Linux dan Windows dan menyebarkan aplikasi Windows di Cloud AWS.
- Kebanyakan aplikasi dan alat-alat yang Anda gunakan hari ini yang memerlukan dukungan Microsoft Active Directory dapat digunakan dengan Simple AD.
- Akun pengguna di Simple AD memungkinkan akses ke AWS aplikasi seperti WorkSpaces, Amazon WorkDocs, atau Amazon WorkMail.
- Anda dapat mengelola sumber daya AWS melalui akses berbasis IAM role ke AWS Management Console.
- Snapshot otomatis harian memungkinkan point-in-time pemulihan.

Simple AD tidak mendukung berikut ini:

- Amazon AppStream 2.0
- Amazon Chime
- Amazon RDS for SQL Server

- Amazon RDS for Oracle
- AWS IAM Identity Center
- Hubungan Kepercayaan dengan domain lain
- Pusat Administrasi Direktori Aktif
- PowerShell
- Keranjang sampah Direktori Aktif
- Akun layanan yang dikelola grup
- Ekstensi skema untuk aplikasi POSIX dan Microsoft

Lanjutkan membaca topik di bagian ini untuk mempelajari cara membuat Simple AD Anda sendiri.

Topik

Memulai dengan Simple AD

Simple AD membuat direktori berbasis Samba yang dikelola sepenuhnya di cloud. AWS Saat Anda membuat direktori dengan Simple AD, AWS Directory Service buat dua pengontrol domain dan server DNS atas nama Anda. Pengontrol domain dibuat dalam subnet yang berbeda di VPC Amazon, redundansi ini membantu memastikan bahwa direktori Anda tetap dapat diakses bahkan jika terjadi kegagalan.

Topik

- Konfigurasikan DNS untuk Simple AD

Prasyarat Simple AD

Untuk membuat Simple AD Active Directory, Anda memerlukan VPC Amazon dengan yang berikut ini:

- VPC harus memiliki penghunian perangkat keras default.
- VPC tidak boleh dikonfigurasi dengan VPC endpoint berikut:
  - Titik akhir VPC Route53 yang menyertakan penggantian bersyarat DNS untuk*.amazonaws.com yang menyelesaikan ke alamat IP non publik AWS
  - CloudWatch Titik akhir VPC
  - Titik akhir VPC Systems Manager
  - Titik akhir VPC Layanan Token Keamanan
- Setidaknya dua subnet di dua Availability Zone yang berbeda. Subnet harus berada dalam rentang Classless Inter-Domain Routing (CIDR) yang sama. Jika Anda ingin memperpanjang atau mengubah ukuran VPC untuk direktori Anda, maka pastikan untuk memilih kedua subnet pengendali domain untuk rentang VPC CIDR yang diperpanjang. Saat Anda membuat Simple AD, AWS Directory Service buat dua pengontrol domain dan server DNS atas nama Anda.
  - Untuk informasi selengkapnya tentang rentang CIDR, lihat pengalamatan IP untuk VPC dan subnet Anda di Panduan Pengguna Amazon VPC.
- Jika Anda memerlukan dukungan LDAPS dengan Simple AD, kami sarankan Anda mengonfigurasinya menggunakan Network Load Balancer yang terhubung ke port 389. Model ini memungkinkan Anda untuk menggunakan sertifikat yang kuat untuk hubungan LDAPS, menyederhanakan akses ke LDAPS melalui alamat IP NLB tunggal, dan memiliki kegagalan otomatis melalui NLB. Simple AD tidak mendukung penggunaan sertifikat yang ditandatangani sendiri pada port 636. Untuk informasi selengkapnya tentang cara mengkonfigurasi LDAPS dengan Simple AD, lihat Cara mengkonfigurasi titik akhir LDAPS untuk Simple AD di Blog Keamanan AWS .
- Jenis enkripsi berikut harus diaktifkan dalam direktori:
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1
  - AES256_HMAC_SHA1
  - Jenis enkripsi masa depan

> **Note**
>
> Menonaktifkan jenis enkripsi ini dapat menyebabkan masalah komunikasi dengan RSAT (Remote Server Administration Tools) dan mempengaruhi ketersediaan atau direktori Anda.

- Untuk informasi lebih lanjut, lihat Apa itu Amazon VPC? di Panduan Pengguna Amazon VPC.

AWS Directory Service menggunakan dua struktur VPC. Instans EC2 yang membentuk direktori Anda berjalan di luar AWS akun Anda, dan dikelola oleh. AWS Mereka memiliki dua adaptor jaringan, `ETH0` dan `ETH1`. `ETH0` adalah adaptor pengelola, dan berada di luar akun Anda. `ETH1` dibuat dalam akun Anda.

Rentang IP pengelola jaringan `ETH0` direktori Anda dipilih secara terprogram untuk memastikan tidak bertentangan dengan VPC tempat direktori Anda di-deploy. Rentang IP ini dapat berupa salah satu pasangan berikut (karena Direktori berjalan di dua subnet):

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

Kami menghindari konflik dengan memeriksa oktet pertama dari `ETH1` CIDR. Jika dimulai dengan 10, maka kami memilih VPC 192.168.0.0/16 dengan subnet 192.168.1.0/24 dan 192.168.2.0/24. Jika oktet pertama adalah yang lain selain 10, kami memilih VPC 10.0.0.0/16 dengan subnet 10.0.1.0/24 dan 10.0.2.0/24.

Algoritma pemilihan tidak mencakup rute pada VPC Anda. Oleh karena itu Anda dapat mengalami konflik IP perutean yang dihasilkan dari skenario ini.

Buat Direktori Aktif AD Sederhana Anda

Untuk membuat Simple AD baruActive Directory, lakukan langkah-langkah berikut. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan prasyarat yang diidentifikasi dalam Prasyarat Simple AD.

Untuk membuat Simple AD Active Directory

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori, lalu pilih Atur direktori.
2. Di halaman Pilih jenis direktori, pilih Simple AD, lalu pilih Selanjutnya.
3. Di halaman Masukkan informasi direktori, berikan informasi berikut:

   Ukuran direktori

   Pilih salah satu opsi ukuran Small atau Large. Untuk informasi selengkapnya tentang ukuran, lihat Simple AD.

   Nama organisasi

   Sebuah nama organisasi yang unik untuk direktori Anda yang akan digunakan untuk mendaftarkan perangkat klien.

   Bidang ini hanya tersedia jika Anda membuat direktori sebagai bagian dari peluncuran WorkSpaces.

   Nama DNS direktori

   Nama berkualifikasi penuh untuk direktori, seperti `corp.example.com`.

   Direktori nama NetBIOS

   Nama singkat untuk direktori, seperti `CORP`.

   Kata sandi administrator

   Kata sandi administrator direktori. Proses pembuatan direktori menciptakan akun administrator dengan nama pengguna `Administrator` dan kata sandi ini.

   Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

   - Huruf kecil (a-z)
   - Huruf besar (A-Z)
   - Angka (0-9)
   - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

   Konfirmasikan kata sandi

   Ketik ulang kata sandi administrator.

Deskripsi direktori

Deskripsi opsional untuk direktori.

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

   VPC

   VPC untuk direktori.

   Subnet

   Pilih subnet untuk pengendali domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.

5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Ini akan memerlukan beberapa menit sampai direktori dibuat. Setelah dibuat, nilai Status berubah ke Aktif.

Apa yang dibuat dengan Simple AD Active Directory

Saat Anda membuat Direktori Aktif dengan Simple AD, AWS Directory Service lakukan tugas-tugas berikut atas nama Anda:

- Mengatur direktori berbasis Samba dalam VPC.
- Membuat akun administrator direktori dengan nama pengguna `Administrator` dan kata sandi yang ditentukan. Anda menggunakan akun ini untuk mengelola direktori.

  Important

  Pastikan untuk menyimpan kata sandi ini. AWS Directory Service tidak menyimpan kata sandi ini, dan tidak dapat diambil. Namun, Anda dapat mengatur ulang kata sandi dari AWS Directory Service konsol atau dengan menggunakan ResetUserPasswordAPI.

- Membuat grup keamanan untuk pengontrol direktori.
- Membuat akun dengan nama `AWSAdminD-`*`xxxxxxxx`* yang memiliki hak istimewa admin domain. Akun ini digunakan oleh AWS Directory Service untuk melakukan operasi otomatis untuk operasi pemeliharaan direktori, seperti mengambil snapshot direktori dan transfer peran FSMO. Kredensial untuk akun ini disimpan dengan aman oleh AWS Directory Service.

- Secara otomatis membuat dan mengasosiasikan antarmuka jaringan elastis (ENI) dengan masing-masing pengendali domain Anda. Masing-masing ENI ini penting untuk konektivitas antara VPC AWS Directory Service dan pengontrol domain Anda dan tidak boleh dihapus. Anda dapat mengidentifikasi semua antarmuka jaringan yang dicadangkan untuk digunakan AWS Directory Service dengan deskripsi: "AWS menciptakan antarmuka jaringan untuk direktori-id direktori". Untuk informasi selengkapnya, lihat Antarmuka Jaringan Elastis di Panduan Pengguna Amazon EC2 untuk Instans Windows. Server DNS default dari Microsoft AD yang AWS Dikelola Active Directory adalah server DNS VPC di Classless Inter-Domain Routing (CIDR) +2. Untuk informasi selengkapnya, lihat Server DNS Amazon di Panduan Pengguna Amazon VPC.

> **Note**
>
> Pengendali domain di-deploy di dua Availability Zone di suatu Region secara default dan terhubung ke Amazon Virtual Private Cloud (VPC) Anda. Backup secara otomatis diambil sekali per hari, dan volume Amazon Elastic Block Store (EBS) dienkripsi untuk memastikan bahwa data diamankan saat istirahat. Pengendali domain yang gagal secara otomatis diganti di Availability Zone yang sama menggunakan alamat IP yang sama, dan pemulihan bencana penuh dapat dilakukan dengan menggunakan backup terbaru.

Konfigurasikan DNS untuk Simple AD

Simple AD meneruskan permintaan DNS ke alamat IP server DNS yang disediakan Amazon untuk VPC Amazon Anda. Server DNS ini akan menyelesaikan nama yang dikonfigurasi di zona host pribadi Amazon Route 53 Anda. Dengan mengarahkan komputer on-premise ke Simple AD Anda, Anda sekarang dapat menyelesaikan permintaan DNS ke zona yang di-hosting pribadi. Untuk informasi selengkapnya tentang Route 53, lihat Apa itu Route 53.

Perhatikan bahwa untuk mengaktifkan Simple AD untuk menanggapi permintaan DNS eksternal, access control list (ACL) jaringan untuk VPC yang berisi Simple AD Anda harus dikonfigurasi untuk mengizinkan lalu lintas dari luar VPC.

- Jika Anda tidak menggunakan Route 53 zona yang di-hosting pribadi, permintaan DNS Anda akan diteruskan ke server DNS publik.
- Jika Anda menggunakan server DNS kustom yang berada di luar VPC Anda dan Anda ingin menggunakan DNS pribadi, Anda harus mengkonfigurasi ulang untuk menggunakan server DNS kustom pada instans EC2 dalam VPC Anda. Untuk informasi selengkapnya, lihat Bekerja dengan zona yang di-hosting pribadi.

- Jika Anda ingin Simple AD untuk menyelesaikan nama menggunakan kedua server DNS dalam VPC Anda dan server DNS pribadi di luar VPC Anda, Anda dapat melakukannya menggunakan set opsi DHCP. Untuk contoh terperinci, lihat artikel ini.

> **Note**
>
> Pembaruan dinamis DNS tidak didukung di domain Simple AD. Sebagai gantinya Anda dapat membuat perubahan secara langsung dengan menghubungkan ke direktori Anda menggunakan Pengelola DNS pada instans yang digabungkan ke domain Anda.

Cara mengelola Simple AD

Bagian ini berisi daftar semua prosedur untuk mengoperasikan dan memelihara lingkungan Simple AD.

Topik

Mengelola pengguna dan grup di Simple AD

Pengguna mewakili individu orang atau entitas yang memiliki akses ke direktori Anda. Grup sangat berguna untuk memberikan atau menolak hak istimewa ke grup pengguna, daripada harus menerapkan hak istimewa tersebut ke setiap pengguna. Jika pengguna berpindah ke organisasi yang berbeda, Anda memindahkan pengguna tersebut ke grup yang berbeda dan mereka secara otomatis menerima hak istimewa yang diperlukan untuk organisasi baru.

Untuk membuat pengguna dan grup di direktori AWS Directory Service, Anda harus menggunakan instans apapun (dari on-premise atau EC2) yang telah bergabung ke direktori AWS Directory Service Anda, dan masuk sebagai pengguna yang memiliki hak istimewa untuk membuat pengguna dan

grup. Anda juga perlu menginstal Alat Direktori Aktif pada instans EC2 Anda sehingga Anda dapat menambahkan pengguna dan grup dengan snap-in Pengguna dan Komputer Direktori Aktif. Untuk informasi selengkapnya tentang cara mengatur instans EC2 dan menginstal alat yang diperlukan, lihat Bergabunglah dengan instans Amazon EC2 ke Simple AD Active Directory.

> **Note**
>
> Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, tetapi tidak boleh diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka Preauthentication di Microsoft. TechNet

Topik berikut termasuk petunjuk tentang cara membuat dan mengelola pengguna dan grup.

Topik

- Instal Alat Administrasi Direktori Aktif untuk Simple AD
- Buat pengguna
- Hapus pengguna
- Mengatur ulang kata sandi pengguna
- Membuat grup
- Menambahkan pengguna ke grup

Instal Alat Administrasi Direktori Aktif untuk Simple AD

Untuk mengelola Active Directory dari instans Amazon EC2 Windows Server, Anda perlu menginstal Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools pada instans. Gunakan prosedur berikut untuk menginstal alat-alat ini pada instance EC2 Windows Server.

Prasyarat

Sebelum Anda dapat memulai prosedur ini, selesaikan yang berikut ini:

1. Buat Direktori Aktif AD Sederhana. Untuk informasi selengkapnya, lihat Buat Direktori Aktif AD Sederhana Anda.
2. Luncurkan dan gabungkan instans Windows Server EC2 ke Simple AD Active Directory Anda. Instans EC2 memerlukan kebijakan berikut untuk membuat pengguna dan grup: **`AWSSSMManagedInstanceCore`** dan**`AmazonSSMDirectoryServiceAccess`**. Untuk informasi

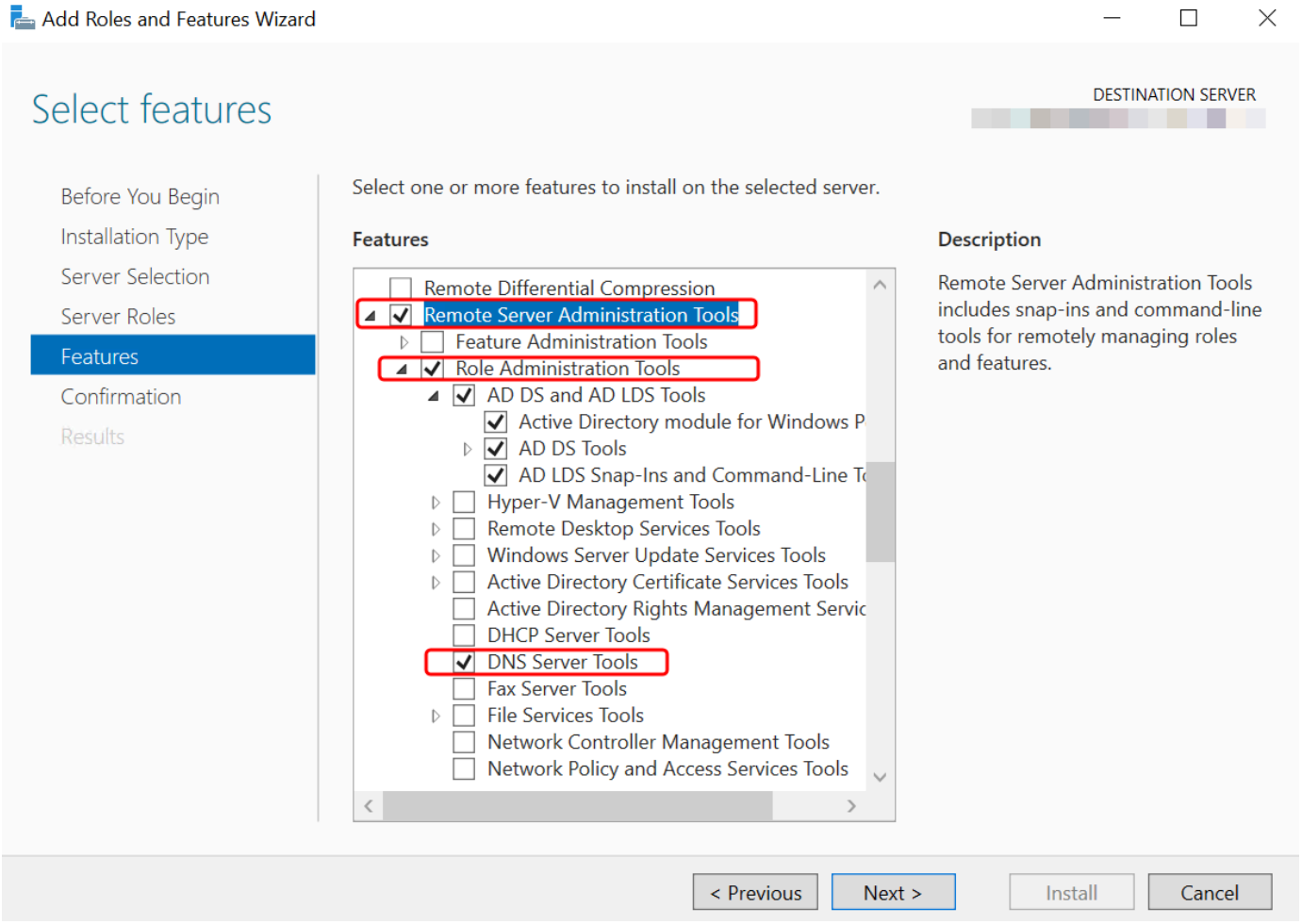
selengkapnya, lihat Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Simple AD Active Directory.

3. Anda akan memerlukan kredensi untuk Administrator domain Direktori Aktif Anda. Kredensi ini dibuat ketika Simple AD dibuat. Jika Anda mengikuti prosedur diBuat Direktori Aktif AD Sederhana Anda, nama pengguna Administrator Anda menyertakan nama NetBIOS Anda,. **corp\administrator**

Instal Alat Administrasi Direktori Aktif pada instans Windows Server EC2

Untuk menginstal alat administrasi Direktori Aktif pada instans EC2 Windows Server

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di konsol Amazon EC2, pilih Instans, pilih instance Windows Server, lalu pilih Connect.
3. Di halaman Connect to instance, pilih klien RDP.
4. Di tab klien RDP, pilih Unduh File Desktop Jarak Jauh, lalu pilih Dapatkan Kata Sandi untuk mengambil kata sandi Anda.
5. Dalam kata sandi Dapatkan Windows, pilih Unggah file kunci pribadi. Pilih file kunci pribadi.pem yang terkait dengan instance Windows Server. Setelah mengunggah file kunci pribadi, pilih Dekripsi kata sandi.
6. Di kotak dialog Keamanan Windows, salin kredensi administrator lokal Anda untuk komputer Windows Server untuk masuk. Nama pengguna dapat dalam format berikut: ***NetBIOS-Name*\administrator** atau***DNS-Name*\administrator**. Misalnya, **corp\administrator** akan menjadi nama pengguna jika Anda mengikuti prosedur diBuat Direktori Aktif AD Sederhana Anda.
7. Setelah masuk ke instance Windows Server, buka Server Manager dari menu Start dengan memilih Server Manager.
8. Di Dasbor Manajer Server, pilih Tambahkan peran dan fitur.
9. Di Tambahkan peran dan fitur Wizard pilih Jenis Instalasi, pilih Instalasi berbasis peran atau berbasis fitur, dan pilih Selanjutnya.
10. Di bawah Pilihan Server, pastikan server lokal dipilih, dan pilih Fitur di panel navigasi sebelah kiri.
11. Di pohon Fitur, pilih dan buka Alat Administrasi Server Jarak Jauh, Alat Administrasi Peran, dan Alat AD DS dan AD LDS. Dengan AD DS dan AD LDS Tools dipilih, Active Directorymodul untuk, AD DS ToolsWindows PowerShell, dan AD LDS Snap-in dan Command-Line Tools dipilih. Gulir ke bawah dan pilih DNS Server Tools, lalu pilih Berikutnya.



12. Tinjau informasi dan pilih Instal. Ketika instalasi fitur selesai, Active Directory Domain Services dan Active Directory Lightweight Directory Services Tools tersedia dari menu Start di folder Administrative Tools.

Metode Alternatif untuk menginstal Alat Administrasi Direktori Aktif pada instans Server Windows EC2

- Berikut adalah metode lain untuk menginstal Alat Administrasi Direktori Aktif:
  - Anda dapat memilih untuk menginstal alat administrasi Direktori Aktif menggunakanWindows PowerShell. Misalnya, Anda dapat menginstal alat administrasi jarak jauh Active Directory dari PowerShell prompt menggunakan`Install-WindowsFeature RSAT-ADDS`. Untuk informasi selengkapnya, lihat Menginstal- WindowsFeature di situs web Microsoft.

Buat pengguna

Gunakan prosedur berikut untuk membuat pengguna dengan instans EC2 yang digabungkan ke direktori Simple AD Anda. Sebelum Anda dapat membuat pengguna, Anda harus menyelesaikan prosedur di Instalasi Alat Administrasi Direktori Aktif.

> **Note**
>
> Saat menggunakan Simple AD, jika Anda membuat akun pengguna pada instans Linux dengan opsi “Paksa pengguna untuk mengubah kata sandi saat login pertama,” pengguna tersebut tidak akan dapat mengubah kata sandi mereka menggunakan kpasswd. Untuk mengubah kata sandi pertama kalinya, administrator domain harus memperbarui sandi pengguna menggunakan Alat Pengelolaan Direktori Aktif.

Anda dapat menggunakan salah satu metode berikut untuk membuat pengguna:

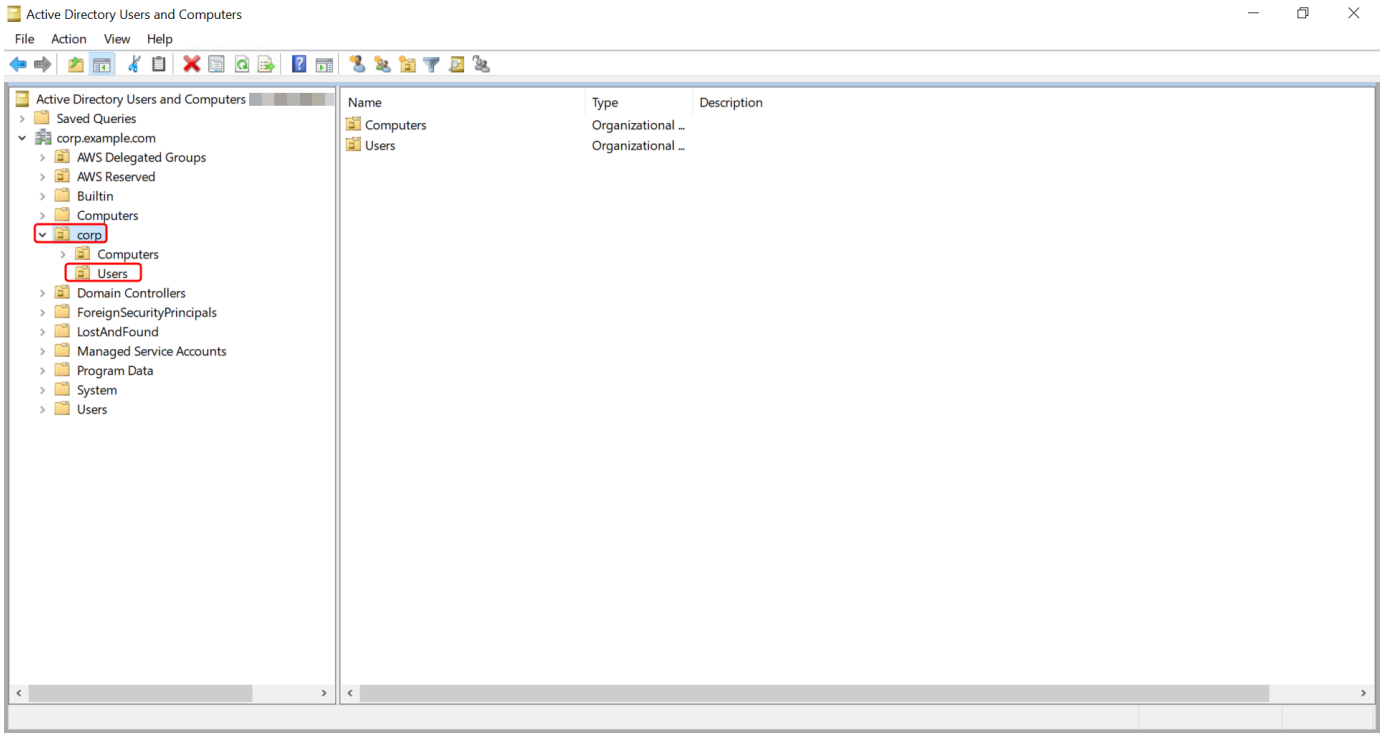
- Active DirectoryAlat Administrasi
- Windows PowerShell

Buat pengguna dengan Alat Active Directory Administrasi

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Active Directory Users and Computers dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

   > **Tip**
   >
   > Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Di pohon direktori, pilih OU di bawah nama NetBIOS direktori Anda OU di mana Anda ingin menyimpan pengguna Anda (misalnya,**`corp\Users`**). Untuk informasi lebih lanjut tentang struktur OU yang digunakan oleh direktori di AWS, lihatApa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.



4. Pada menu Tindakan, pilih Baru, lalu pilih Pengguna untuk membuka wizard pengguna baru.
5. Pada halaman pertama wizard, masukkan nilai untuk bidang berikut, lalu pilih Berikutnya.
   - Nama depan
   - Nama belakang
   - Nama logon pengguna
6. Pada halaman kedua wizard, masukkan kata sandi sementara di Kata Sandi dan Konfirmasi Kata Sandi. Pastikan pilihan Pengguna harus mengubah kata sandi pada proses masuk berikutnya dipilih. Tidak satu pun dari pilihan lain harus dipilih. Pilih Berikutnya.
7. Pada halaman ketiga wizard, verifikasi bahwa informasi pengguna baru sudah benar dan pilih Selesai. Pengguna baru akan muncul di folder Pengguna.

Buat pengguna di Windows PowerShell

1. Connect ke instance yang bergabung dengan Active Directory domain Anda sebagai Active Directory administrator.
2. Buka Windows PowerShell.
3. Ketik perintah berikut mengganti nama pengguna **`jane.doe`** dengan nama pengguna pengguna yang ingin Anda buat. Anda akan diminta Windows PowerShell untuk memberikan kata sandi

untuk pengguna baru. Untuk informasi selengkapnya tentang persyaratan kompleksitas Active Directory kata sandi, lihat Microsoftdokumentasi. Untuk informasi selengkapnya tentang perintah New-aduser, lihat dokumentasi. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Hapus pengguna

Gunakan prosedur berikut untuk menghapus pengguna dengan instans EC2 Windows yang bergabung ke direktori Simple AD Anda.

Anda dapat menggunakan salah satu metode berikut untuk menghapus pengguna:

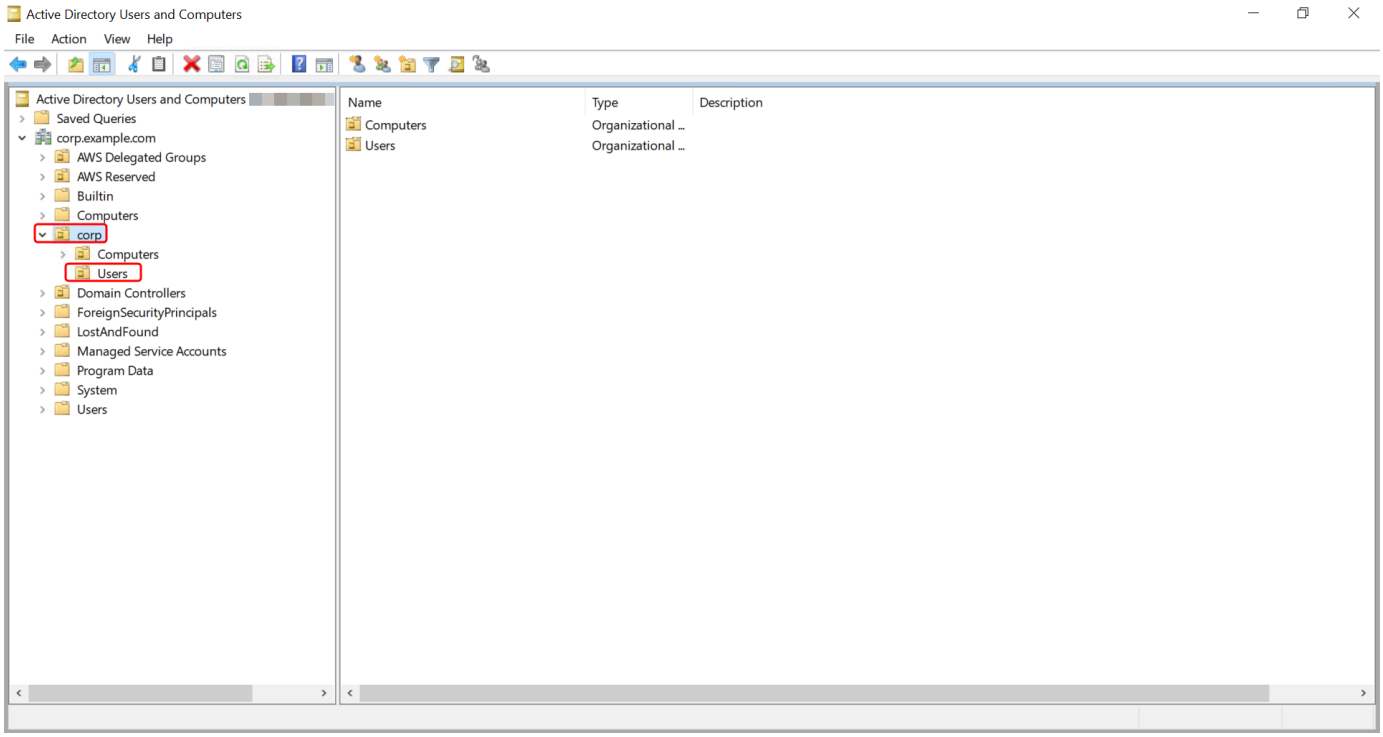
- Active DirectoryAlat Administrasi
- Windows PowerShell

Hapus pengguna dengan Alat Active Directory Administrasi

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif dari menu Start Windows. Ada pintasan ke alat ini yang ditemukan di folder Alat Administratif Windows.

   > **Tip**
   >
   > Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Di pohon direktori, pilih OU yang berisi pengguna yang ingin Anda hapus (misalnya,**`corp\Users`**).



4. Pilih pengguna yang ingin Anda hapus. Pada menu Tindakan, pilih Hapus.
5. Kotak dialog akan muncul meminta Anda untuk mengonfirmasi bahwa Anda ingin menghapus pengguna. Pilih Ya untuk menghapus pengguna. Ini menghapus pengguna yang dipilih secara permanen.

Hapus pengguna di Windows PowerShell

1. Connect ke instance yang bergabung dengan Active Directory domain Anda sebagai Active Directory administrator.
2. Buka Windows PowerShell.
3. Ketik perintah berikut mengganti nama pengguna **`jane.doe`** dengan nama pengguna pengguna yang ingin Anda hapus. Untuk informasi selengkapnya tentang perintah Remove-aduser, lihat dokumentasi. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Mengatur ulang kata sandi pengguna

Pengguna harus mematuhi kebijakan kata sandi sebagaimana didefinisikan dalamActive Directory. Terkadang ini bisa mendapatkan yang terbaik dari pengguna, termasuk Active Directory administrator, dan mereka lupa kata sandi mereka. Ketika ini terjadi, Anda dapat dengan cepat mengatur ulang kata sandi pengguna menggunakan AWS Directory Service jika pengguna berada di Simple AD.

Anda harus masuk sebagai pengguna dengan izin yang diperlukan untuk mengatur ulang kata sandi. Untuk informasi selengkapnya tentang izin, lihat Ikhtisar mengelola izin akses ke sumber daya Anda AWS Directory Service.

Anda dapat mengatur ulang kata sandi untuk setiap pengguna di Anda Active Directory dengan pengecualian berikut:

- Anda dapat mengatur ulang kata sandi untuk setiap pengguna dalam Unit Organisasi (OU) yang didasarkan dari nama NetBIOS yang Anda gunakan saat Anda membuat. Active Directory Misalnya, jika Anda mengikuti prosedur diBuat Direktori Aktif AD Sederhana Anda, nama NetBIOS Anda akan menjadi CORP dan kata sandi pengguna yang dapat Anda atur ulang akan menjadi anggota Corp/Users OU.
- Anda tidak dapat mengatur ulang kata sandi pengguna mana pun di luar OU yang didasarkan pada nama NetBIOS yang Anda gunakan saat Anda membuat. Active Directory Untuk informasi selengkapnya tentang struktur OU untuk Simple AD, lihatApa yang dibuat dengan Simple AD Active Directory.
- Anda tidak dapat mengatur ulang kata sandi untuk pengguna mana pun yang merupakan anggota dari dua domain. Anda juga tidak dapat mengatur ulang kata sandi pengguna mana pun yang merupakan anggota dari grup Admin Domain atau Admin Perusahaan kecuali untuk pengguna Administrator.

Anda dapat menggunakan salah satu metode berikut untuk mengatur ulang kata sandi pengguna:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Setel ulang kata sandi pengguna di AWS Management Console

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori, lalu pilih Active Directory dalam daftar tempat Anda ingin mengatur ulang kata sandi pengguna.

2. Pada halaman Detail direktori, pilih Tindakan, lalu pilih Setel ulang kata sandi pengguna.
3. Dalam dialog Reset kata sandi pengguna, di Nama pengguna ketikkan nama pengguna pengguna yang kata sandinya perlu diubah.
4. Ketik kata sandi di Kata sandi baru dan Konfirmasi kata sandi, lalu pilih Atur ulang sandi.

Setel ulang kata sandi pengguna di AWS CLI

1. Untuk menginstal AWS CLI, lihat Menginstal atau memperbarui versi terbaru dari file AWS CLI.
2. Buka AWS CLI.
3. Ketik perintah berikut dan ganti ID Direktori, nama pengguna**`jane.doe`**, dan kata sandi **`P@ssw0rd`** dengan ID Active Directory Direktori Anda dan kredensi yang diinginkan. Lihat reset-user-passworddi Referensi AWS CLI Perintah untuk informasi lebih lanjut.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Setel ulang kata sandi pengguna di Windows PowerShell

1. Connect ke instance yang bergabung dengan Active Directory domain Anda sebagai Active Directory administrator.
2. Buka Windows PowerShell.
3. Ketik perintah berikut mengganti nama pengguna**`jane.doe`**, ID Direktori, dan kata sandi **`P@ssw0rd`** dengan ID Active Directory Direktori Anda dan kredensi yang diinginkan. Lihat Reset-DS UserPassword Cmdlet untuk informasi selengkapnya.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Membuat grup

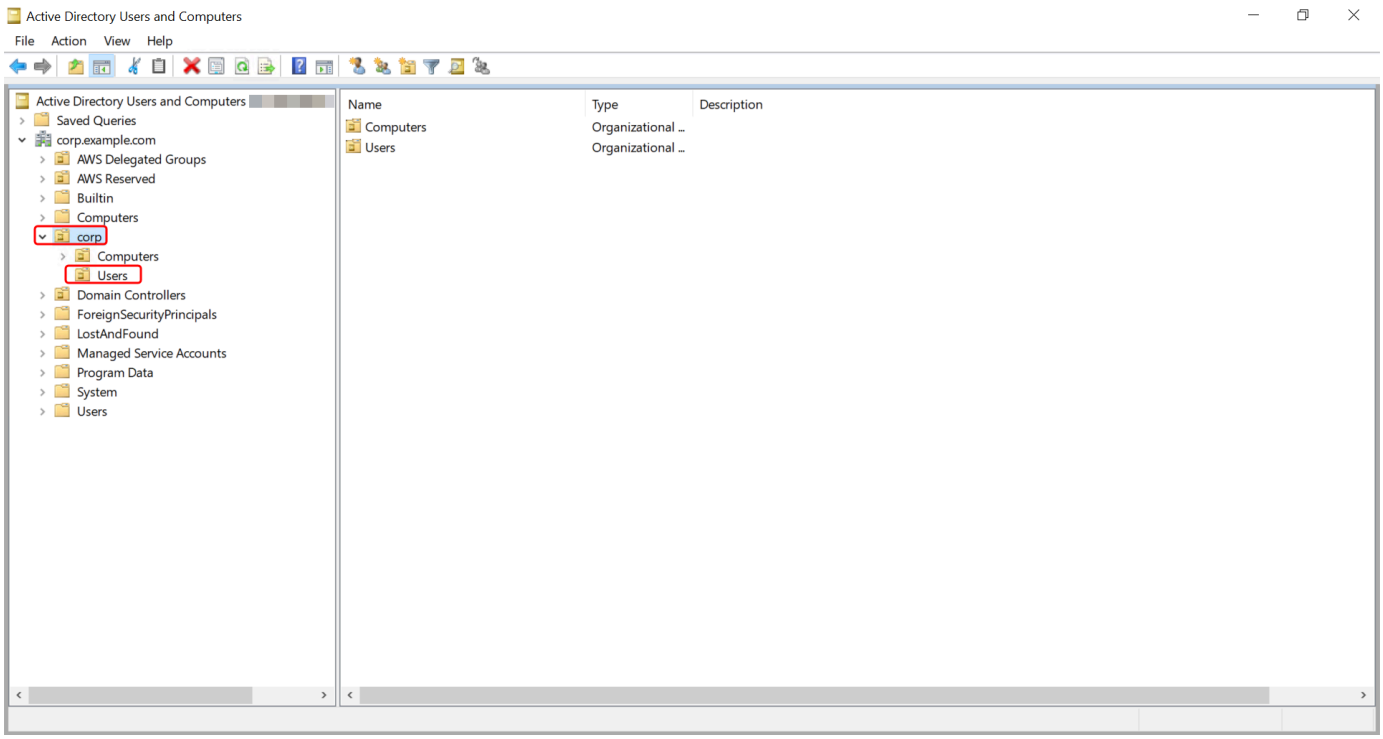
Gunakan prosedur berikut untuk membuat grup keamanan dengan instans EC2 yang digabungkan ke direktori Simple AD Anda. Sebelum Anda dapat membuat grup keamanan, Anda harus menyelesaikan prosedur di Instalasi Alat Administrasi Direktori Aktif.

Untuk membuat grup

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

> **Tip**
>
> Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Pada pohon direktori, pilih OU di bawah direktori OU nama NetBIOS Anda di mana Anda ingin menyimpan grup Anda (misalnya, Corp\Users). Untuk informasi selengkapnya tentang struktur OU yang digunakan oleh direktori di AWS, lihat Apa yang dibuat dengan Direktori Aktif Microsoft AD AWS Terkelola.



4. Pada menu Tindakan, klik Baru, dan kemudian klik Grup untuk membuka wizard grup baru.
5. Ketik nama untuk grup di Nama grup, pilih Lingkup grup yang memenuhi kebutuhan Anda, dan pilih Keamanan untuk jenis Grup. Untuk informasi selengkapnya tentang lingkup grup Active

Directory dan grup keamanan, lihat Grup keamanan Active Directory di dokumentasi Microsoft Windows Server.

6. Klik OK. Grup keamanan baru akan muncul di folder Pengguna.

Menambahkan pengguna ke grup

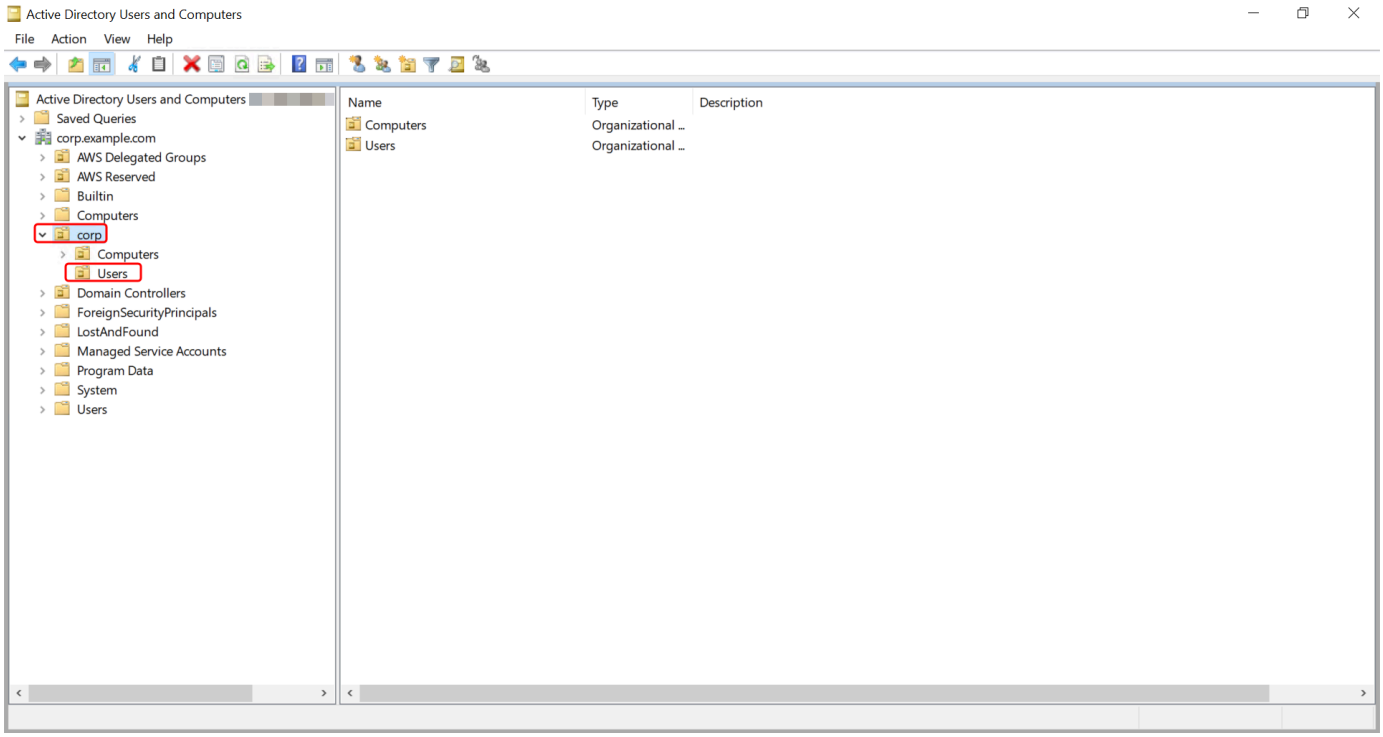
Gunakan prosedur berikut untuk menambahkan pengguna ke grup keamanan dengan instans EC2 yang digabungkan ke direktori Simple AD Anda.

Untuk menambahkan pengguna ke grup

1. Connect ke instance di mana Active Directory Administration Tools diinstal.
2. Buka alat Pengguna dan Komputer Direktori Aktif. Ada jalan pintas untuk alat ini di folder Alat Administratif.

> **Tip**
>
> Anda dapat menjalankan hal berikut dari prompt perintah pada instans untuk membuka kotak alat Pengguna dan Komputer Direktori Aktif secara langsung.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Pada pohon direktori, pilih OU di bawah direktori Anda NetBIOS nama OU di mana Anda disimpan grup Anda, dan pilih grup yang Anda ingin tambahkan pengguna sebagai anggota.



4. Pada menu Tindakan, klik Properti untuk membuka kotak dialog properti untuk grup.
5. Pilih tab Anggota dan klik Tambahkan.
6. Untuk Masukkan nama objek yang akan dipilih, ketik nama pengguna yang ingin Anda tambahkan dan klik OK. Nama akan ditampilkan dalam daftar Anggota. Klik OK lagi untuk memperbarui keanggotaan grup.
7. Verifikasikan bahwa pengguna tersebut sekarang adalah anggota grup dengan memilih pengguna di folder Pengguna dan klik Properti di menu Tindakan untuk membuka kotak dialog properti. Pilih tab Anggota dari. Anda harus melihat nama grup dalam daftar grup yang dimiliki pengguna.

Memantau direktori Simple AD

Anda dapat memantau direktori Simple AD Anda dengan metode berikut:

Topik

- Memahami status direktori Anda
- Konfigurasikan pemberitahuan status direktori dengan Amazon SNS

Memahami status direktori Anda

Berikut ini adalah berbagai status untuk direktori.

Aktif

Direktori beroperasi secara normal. Tidak ada masalah yang terdeteksi oleh AWS Directory Service untuk direktori Anda.

Creating

Direktori saat ini sedang dibuat. Pembuatan direktori biasanya memakan waktu antara 20 sampai 45 menit tetapi dapat bervariasi tergantung pada beban sistem.

Dihapus

Direktori telah dihapus. Semua sumber daya untuk direktori telah dirilis. Setelah direktori memasuki keadaan ini, direktori tidak dapat dipulihkan.

Deleting

Direktori saat ini sedang dihapus. Direktori akan tetap dalam keadaan ini sampai benar-benar dihapus. Setelah direktori memasuki keadaan ini, operasi hapus tidak dapat dibatalkan, dan direktori tidak dapat dipulihkan.

Failed

Direktori tidak dapat dibuat. Harap hapus direktori ini. Jika masalah ini berlanjut, hubungi PusatAWS Support.

Terganggu

Direktori berjalan dalam keadaan terdegradasi. Satu atau lebih masalah telah terdeteksi, dan tidak semua operasi direktori dapat bekerja pada kapasitas operasional penuh. Terdapat banyak potensi alasan untuk keadaan direktori seperti ini. Ini termasuk aktivitas pemeliharaan operasional normal seperti patching atau rotasi instans EC2, hot spotting sementara oleh aplikasi pada salah satu pengendali domain Anda, atau perubahan yang Anda buat ke jaringan Anda yang secara tidak sengaja mengganggu komunikasi direktori. Untuk informasi selengkapnya, lihat salah satu dari Pemecahan Masalah AWS Microsoft AD yang Dikelola, Memecahkan masalah AD Connector, Pemecahan masalah Simple AD. Untuk masalah terkait pemeliharaan normal, AWS selesaikan masalah ini dalam waktu 40 menit. Jika setelah meninjau topik pemecahan masalah, direktori Anda dalam keadaan Terganggu lebih dari 40 menit, kami merekomendasikan Anda untuk menghubungi PusatAWS Support.

> **Important**
>
> Jangan memulihkan snapshot ketika direktori dalam keadaan Terganggu. Sangatlah jarang pemulihan snapshot diperlukan untuk mengatasi gangguan. Untuk informasi selengkapnya, lihat Snapshot atau pulihkan direktori Anda.

Tidak bisa dioperasikan

Direktori tidak berfungsi. Semua titik akhir direktori telah melaporkan masalah.

Diminta

Permintaan untuk membuat direktori Anda sedang tertunda.

RestoreFailed

Memulihkan direktori dari snapshot gagal. Silakan coba lagi operasi pemulihan. Jika ini berlanjut, cobalah snapshot yang berbeda, atau hubungi AWS Support Pusat.

Memulihkan

Direktori saat ini sedang dipulihkan dari snapshot otomatis atau manual. Memulihkan dari snapshot biasanya memakan waktu beberapa menit, tergantung pada ukuran data direktori dalam snapshot.

Lihat informasi yang lebih lengkap di Alasan status direktori Simple AD.

Konfigurasikan pemberitahuan status direktori dengan Amazon SNS

Menggunakan Amazon Simple Notification Service (Amazon SNS), Anda dapat menerima pesan email atau teks (SMS) saat status direktori Anda berubah. Anda akan diberitahu jika direktori Anda berubah dari status Aktif ke status Terganggu atau Tidak dapat dioperasikan. Anda juga menerima notifikasi ketika direktori kembali ke status Aktif.

Cara kerjanya

Amazon SNS menggunakan “topik” untuk mengumpulkan dan mendistribusikan pesan. Setiap topik memiliki satu atau lebih pelanggan yang menerima pesan yang telah diterbitkan untuk topik tersebut. Dengan menggunakan langkah-langkah di bawah ini, Anda dapat menambahkan AWS Directory Service sebagai penerbit ke topik Amazon SNS. Saat AWS Directory Service mendeteksi perubahan

dalam status direktori Anda, ia menerbitkan pesan ke topik tersebut, yang kemudian dikirim ke pelanggan topik tersebut.

Anda dapat mengaitkan beberapa direktori sebagai penerbit ke satu topik. Anda juga dapat menambahkan pesan status direktori ke topik yang sebelumnya Anda buat di Amazon SNS. Anda memiliki kendali terperinci atas siapa yang dapat menerbitkan dan berlangganan topik. Untuk informasi lengkap tentang Amazon SNS, lihat Apa yang Dimaksud dengan Amazon SNS?.

Untuk mengaktifkan olahpesan SNS untuk direktori Anda

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih Tindakan, dan kemudian pilih Buat notifikasi.
5. Pada halaman Buat notifikasi, pilih Pilih jenis notifikasi, lalu pilih Buat notifikasi baru. Atau, jika Anda sudah memiliki topik SNS yang ada, Anda dapat memilih Mengasosiasikan topik SNS yang ada untuk mengirim pesan status dari direktori ini ke topik tersebut.

   > **Note**
   >
   > Jika Anda memilih Buat notifikasi baru tetapi kemudian menggunakan nama topik yang sama untuk topik SNS yang sudah ada, Amazon SNS tidak membuat topik baru, tetapi hanya menambahkan informasi langganan baru ke topik yang ada.
   > Jika Anda memilih Mengasosiasikan topik SNS yang ada, Anda hanya akan dapat memilih topik SNS yang ada di Region yang sama dengan direktori.

6. Pilih Jenis penerima dan masukkan informasi kontak Penerima. Jika Anda memasukkan nomor telepon untuk SMS, gunakan angka saja. Jangan menyertakan tanda hubung, spasi, atau tanda kurung.
7. (Opsional) Berikan nama untuk topik Anda dan nama tampilan SNS. Nama tampilan adalah nama pendek hingga 10 karakter yang disertakan dalam semua pesan SMS dari topik ini. Bila menggunakan opsi SMS, nama tampilan diperlukan.

   > **Note**
   >
   > Jika Anda masuk menggunakan pengguna IAM atau peran yang hanya memiliki kebijakan DirectoryServiceFullAccessterkelola, nama topik Anda harus dimulai dengan

> “DirectoryMonitoring”. Jika Anda ingin menyesuaikan nama topik Anda lebih lanjut, Anda memerlukan hak istimewa tambahan untuk SNS.

8. Pilih Buat.

Jika Anda ingin menunjuk pelanggan SNS tambahan, seperti alamat email tambahan, antrian Amazon SQS AWS Lambdaatau, Anda dapat melakukan ini dari konsol Amazon SNS.

Untuk menghapus pesan status direktori dari topik

1. Masuk ke AWS Management Console dan buka AWS Directory Service konsol.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pilih tab Pemeliharaan.
4. Di bagian Pemantauan direktori, pilih nama topik SNS dalam daftar, pilih Tindakan, dan kemudian pilih Hapus.
5. Pilih Hapus.

Ini akan menghapus direktori Anda sebagai penerbit untuk topik SNS yang dipilih. Jika Anda ingin menghapus seluruh topik, Anda dapat melakukan ini dari konsol Amazon SNS.

> **Note**
>
> Sebelum menghapus topik Amazon SNS menggunakan konsol SNS, Anda harus memastikan bahwa direktori tidak mengirim pesan status untuk topik tersebut.
> Jika Anda menghapus topik Amazon SNS menggunakan konsol SNS, perubahan ini tidak akan segera tercermin dalam konsol Directory Service. Anda hanya akan diberitahu pada saat direktori menerbitkan notifikasi untuk topik yang dihapus, dalam hal ini Anda akan melihat status diperbarui pada tab Pemantauan direktori yang menunjukkan topik tidak dapat ditemukan.
> Oleh karena itu, untuk menghindari kehilangan pesan status direktori penting, sebelum menghapus topik apa pun yang menerima pesan dari AWS Directory Service, kaitkan direktori Anda dengan topik Amazon SNS yang berbeda.

Bergabunglah dengan instans Amazon EC2 ke Simple AD Active Directory

Anda dapat menggabungkan instans Amazon EC2 dengan mulus ke domain Active Directory Anda saat instans diluncurkan. Untuk informasi selengkapnya, lihat Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Microsoft AD yang AWS Dikelola Active Directory. Anda juga dapat meluncurkan instans EC2 dan menggabungkannya ke Active Directory domain langsung dari AWS Directory Service konsol dengan AWS Systems Manager Automation.

Jika Anda perlu menggabungkan instans EC2 secara manual ke Active Directory domain Anda, Anda harus meluncurkan instance di Wilayah dan grup keamanan atau subnet yang tepat, lalu bergabung dengan instance tersebut ke domain.

Untuk dapat terhubung dari jarak jauh ke instans ini, Anda harus memiliki konektivitas IP ke instans dari jaringan di mana Anda menghubungkannya dari. Dalam kebanyakan kasus, ini mengharuskan gateway internet dilampirkan ke VPC Anda dan instans tersebut memiliki alamat IP publik.

Topik

Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Simple AD Active Directory

Prosedur ini menggabungkan instans Windows Amazon EC2 dengan mulus ke Simple AD Active Directory Anda.

Untuk bergabung dengan instans Windows EC2 dengan mulus

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.

4. Pada halaman Launch an instance, di bawah bagian Nama dan Tag, masukkan nama yang ingin Anda gunakan untuk instans Windows EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih Windows di panel Mulai Cepat. Anda dapat mengubah Windows Amazon Machine Image (AMI) dari daftar dropdown Amazon Machine Image (AMI).
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada.

    a. Untuk membuat key pair baru, pilih Create new key pair.

    b. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format.

    c. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk.

    d. Pilih create key pair.

    e. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

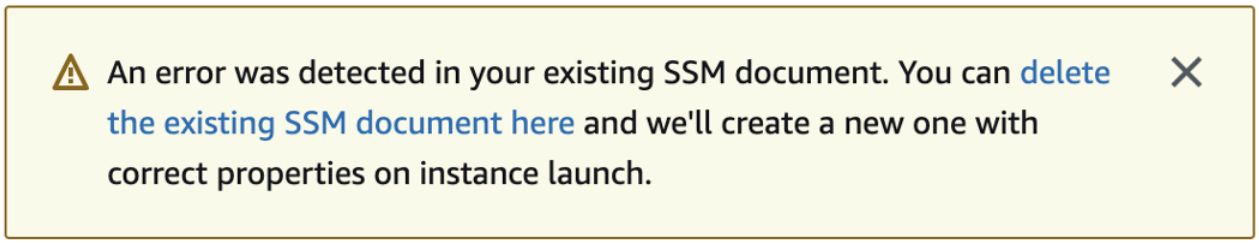
    > **Important**
    >
    > Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.

9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.

12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:
>
> 
>
>
> Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:
>
> - Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
> - Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, Anda dapat memilih profil instans IAM yang ada atau membuat yang baru. Pilih profil instans IAM yang memiliki kebijakan AWS terkelola AmazonSSM ManagedInstanceCore dan AmazonSSM yang DirectoryServiceAccess dilampirkan padanya dari daftar tarik-turun profil instans IAM. Untuk membuat yang baru, pilih Buat tautan profil IAM baru, lalu lakukan hal berikut:

    1. Pilih Buat peran.
    2. Di bawah Pilih entitas tepercaya, pilih AWS layanan.
    3. Di bawah Kasus penggunaan, pilih EC2.

4. Di bawah Tambahkan izin, dalam daftar kebijakan, pilih kebijakan AmazonSSM dan AmazonSSM ManagedInstanceCore. DirectoryServiceAccess Untuk memfilter daftar, **`SSM`** ketik kotak pencarian. Pilih Berikutnya.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

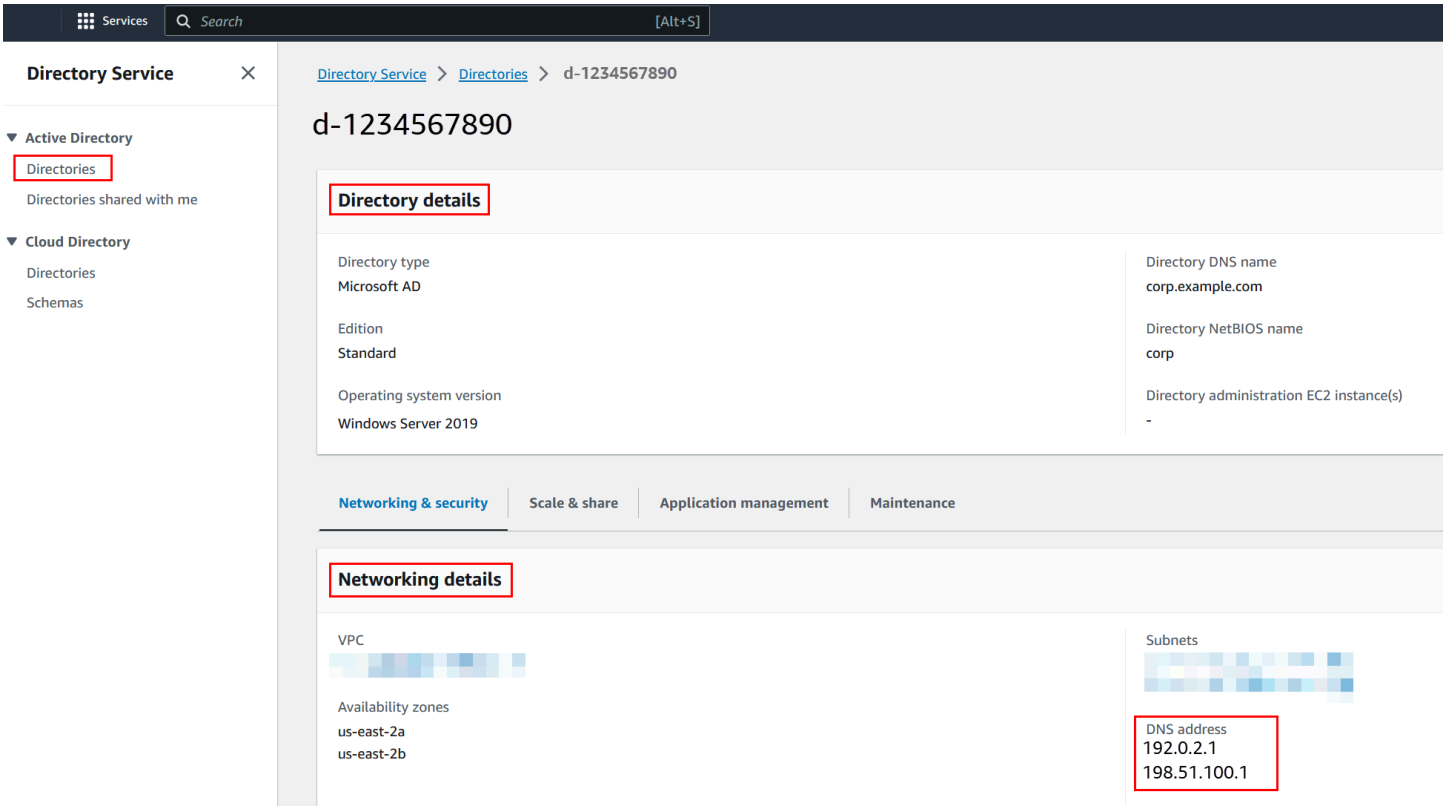
5. Pada halaman Nama, tinjau, dan buat, masukkan nama Peran. Anda akan memerlukan nama peran ini untuk melampirkan ke instans EC2.
6. (Opsional) Anda dapat memberikan deskripsi profil instans IAM di bidang Deskripsi.
7. Pilih Buat peran.
8. Kembali ke Luncurkan halaman instans dan pilih ikon penyegaran di sebelah profil instans IAM. Profil instans IAM baru Anda harus terlihat di daftar dropdown profil instans IAM. Pilih profil baru dan biarkan pengaturan lainnya dengan nilai defaultnya.

16. Pilih Luncurkan instans.

Menggabungkan instans Windows Amazon EC2 secara manual ke Simple AD Active Directory

Untuk menggabungkan instans Windows Amazon EC2 yang ada secara manual ke Simple AD Active Directory, instance harus diluncurkan menggunakan parameter seperti yang ditentukan dalam. Bergabunglah dengan instans Windows Amazon EC2 dengan mulus ke Simple AD Active Directory

Anda akan memerlukan alamat IP dari server DNS Simple AD. Informasi ini dapat ditemukan di bawah Layanan Direktori > Direktori > tautan ID Direktori untuk direktori Anda> Detail direktori dan bagian Jaringan & Keamanan.



Untuk menggabungkan instance Windows ke Simple AD Active Directory

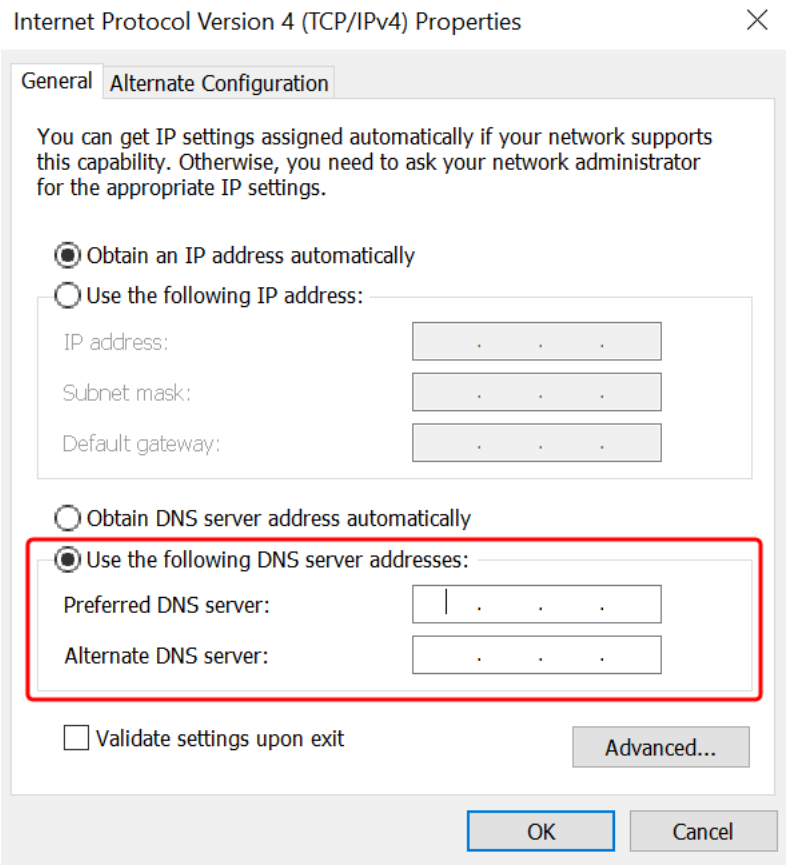
1. Connect ke instans menggunakan klien Remote Desktop Protocol.
2. Buka kotak dialog properti TCP/IPv4 pada instans.

   a. Buka Koneksi Jaringan.

   > **Tip**
   >
   > Anda dapat membuka Koneksi Jaringan langsung dengan menjalankan hal berikut dari prompt perintah pada instans.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Buka menu konteks (klik kanan) untuk koneksi jaringan yang aktif mana pun dan pilih Properti .

   c. Dalam kotak dialog properti koneksi, buka (klik dua kali) Protokol Internet Versi 4.
3. Pilih Gunakan alamat server DNS berikut, ubah server DNS pilihan dan alamat server DNS alternatif ke alamat IP server DNS yang disediakan Iklan Sederhana Anda, dan pilih OK.



4. Buka kotak dialog Properti Sistem untuk instans, pilih tab Nama Komputer, dan pilih Ubah.

> **Tip**
>
> Anda dapat membuka kotak dialog Properti Sistem langsung dengan menjalankan hal berikut dari prompt perintah pada instans.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Di bidang Anggota, pilih Domain, masukkan nama yang sepenuhnya memenuhi syarat dari Simple AD Active Directory Anda, dan pilih OK.
6. Saat diminta nama dan kata sandi untuk administrator domain, masukkan nama pengguna dan kata sandi akun yang memiliki hak istimewa bergabung domain. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Simple AD.

> **Note**
>
> Anda dapat memasukkan nama domain yang sepenuhnya memenuhi syarat atau nama NetBIOS, diikuti dengan garis miring terbalik (\), dan kemudian nama pengguna. Nama pengguna akan menjadi Administrator. Misalnya, **`corp.example.com\administrator`** atau **`corp\administrator`**.

7. Setelah Anda menerima pesan yang menyambut Anda ke domain, mulai ulang instans agar perubahan berlaku.

Sekarang instans Anda telah bergabung ke domain Simple AD Active Directory, Anda dapat masuk ke instance itu dari jarak jauh dan menginstal utilitas untuk mengelola direktori, seperti menambahkan pengguna dan grup. Alat Administrasi Direktori Aktif dapat digunakan untuk membuat pengguna dan grup. Untuk informasi selengkapnya, lihat Instal Alat Administrasi Direktori Aktif untuk Simple AD.

Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory

Prosedur ini menggabungkan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory Anda.

Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Distribusi sebelum Ubuntu 14 dan Red Hat Enterprise Linux 7 tidak mendukung fitur penggabungan domain mulus.

Prasyarat

Sebelum Anda dapat mengatur gabungan domain tanpa batas ke instance Linux, Anda harus menyelesaikan prosedur di bagian ini.

Pilih akun layanan penggabungan domain mulus Anda

Anda dapat menggabungkan komputer Linux secara mulus ke domain Simple AD Anda. Untuk melakukannya, Anda harus membuat akun pengguna dengan membuat izin akun komputer untuk menggabungkan komputer ke domain. Meskipun anggota Admin Domain atau grup lain mungkin memiliki hak istimewa yang memadai untuk menggabungkan komputer ke domain, kami tidak menyarankan untuk menggunakan ini. Sebagai praktik terbaik, kami rekomendasikan Anda menggunakan akun layanan yang memiliki hak istimewa minimum yang diperlukan untuk menggabungkan komputer ke domain.

Untuk informasi tentang cara memproses dan mendelegasikan izin ke akun layanan Anda untuk pembuatan akun komputer, lihat Mendelegasikan hak istimewa ke akun layanan Anda.

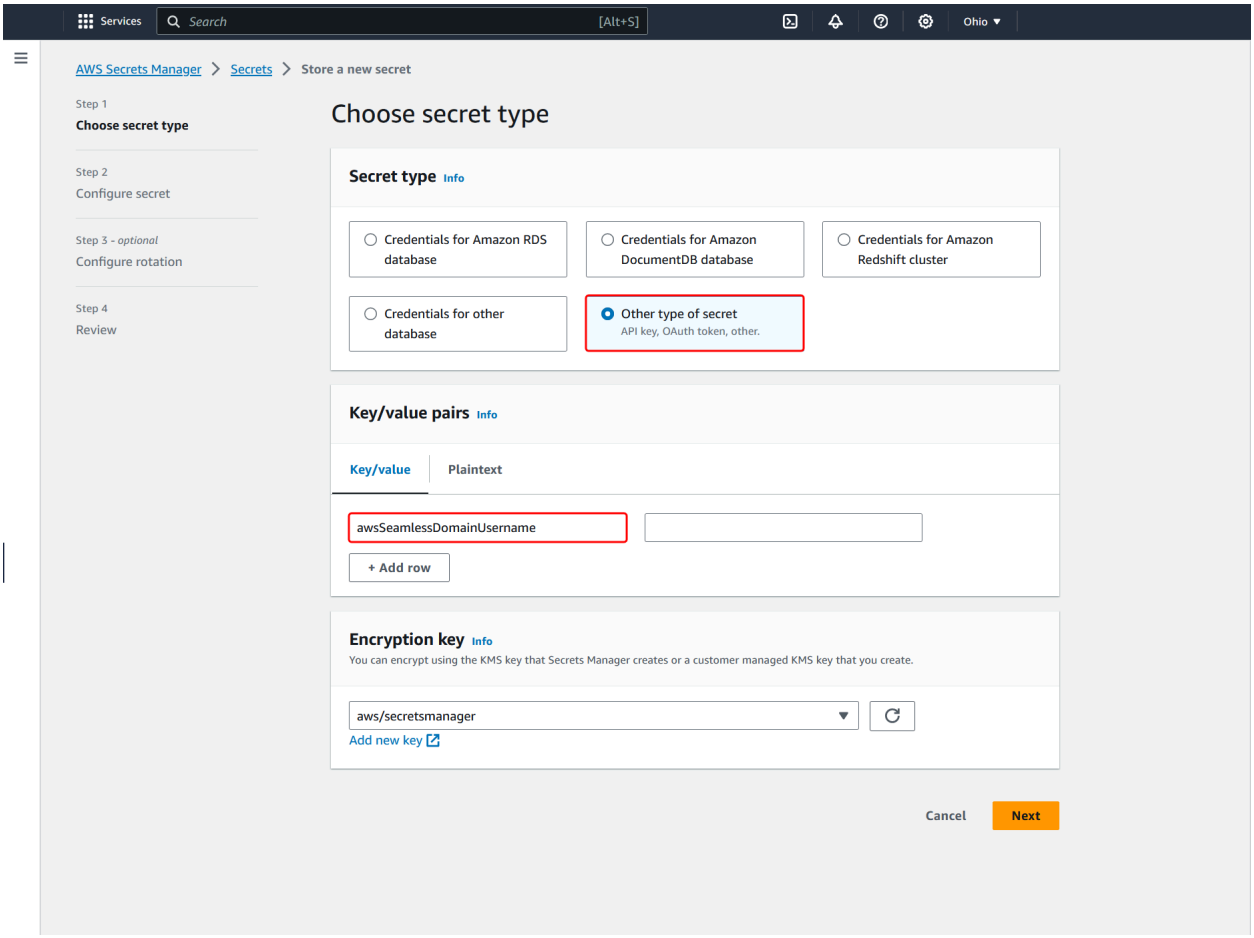
Membuat rahasia untuk menyimpan akun layanan domain

Anda dapat menggunakan AWS Secrets Manager untuk menyimpan akun layanan domain.

Untuk Membuat rahasia dan menyimpan informasi akun layanan domain

1. Masuk ke AWS Management Console dan buka AWS Secrets Manager konsol di https://console.aws.amazon.com/secretsmanager/.
2. Pilih Simpan rahasia baru.
3. Pada halaman Simpan rahasia baru, lakukan hal berikut:
    a. Di bawah Tipe rahasia, pilih Jenis rahasia lainnya.
    b. Di bawah pasangan kunci/nilai, lakukan hal berikut:
        i. Dalam kotak pertama, masukkan **`awsSeamlessDomainUsername`**. Pada baris yang sama, di kotak berikutnya, masukkan nama pengguna untuk akun layanan Anda. Misalnya, jika Anda menggunakan PowerShell perintah sebelumnya, nama akun layanan akan menjadi**`awsSeamlessDomain`**.

> **Note**
>
> Anda harus memasukkan **`awsSeamlessDomainUsername`** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.



ii. Pilih Tambahkan baris.

iii. Pada baris baru, di kotak pertama, masukkan **`awsSeamlessDomainPassword`**. Pada baris yang sama, di kotak berikutnya, masukkan kata sandi untuk akun layanan Anda.

> **Note**
>
> Anda harus memasukkan **awsSeamlessDomainPassword** persis seperti itu. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.

iv. Di bawah kunci Enkripsi, tinggalkan nilai defaultaws/secretsmanager. AWS Secrets Manager selalu mengenkripsi rahasia ketika Anda memilih opsi ini. Anda juga dapat memilih kunci yang Anda buat.

> **Note**
>
> Ada biaya yang terkait AWS Secrets Manager, tergantung pada rahasia yang Anda gunakan. Untuk daftar harga lengkap saat ini, lihat AWS Secrets Manager Harga.
> Anda dapat menggunakan kunci AWS terkelola aws/secretsmanager yang dibuat Secrets Manager untuk mengenkripsi rahasia Anda secara gratis. Jika Anda membuat kunci KMS Anda sendiri untuk mengenkripsi rahasia Anda, AWS menagih Anda dengan tarif saat ini AWS KMS . Untuk informasi selengkapnya, silakan lihat Harga AWS Key Management Service.

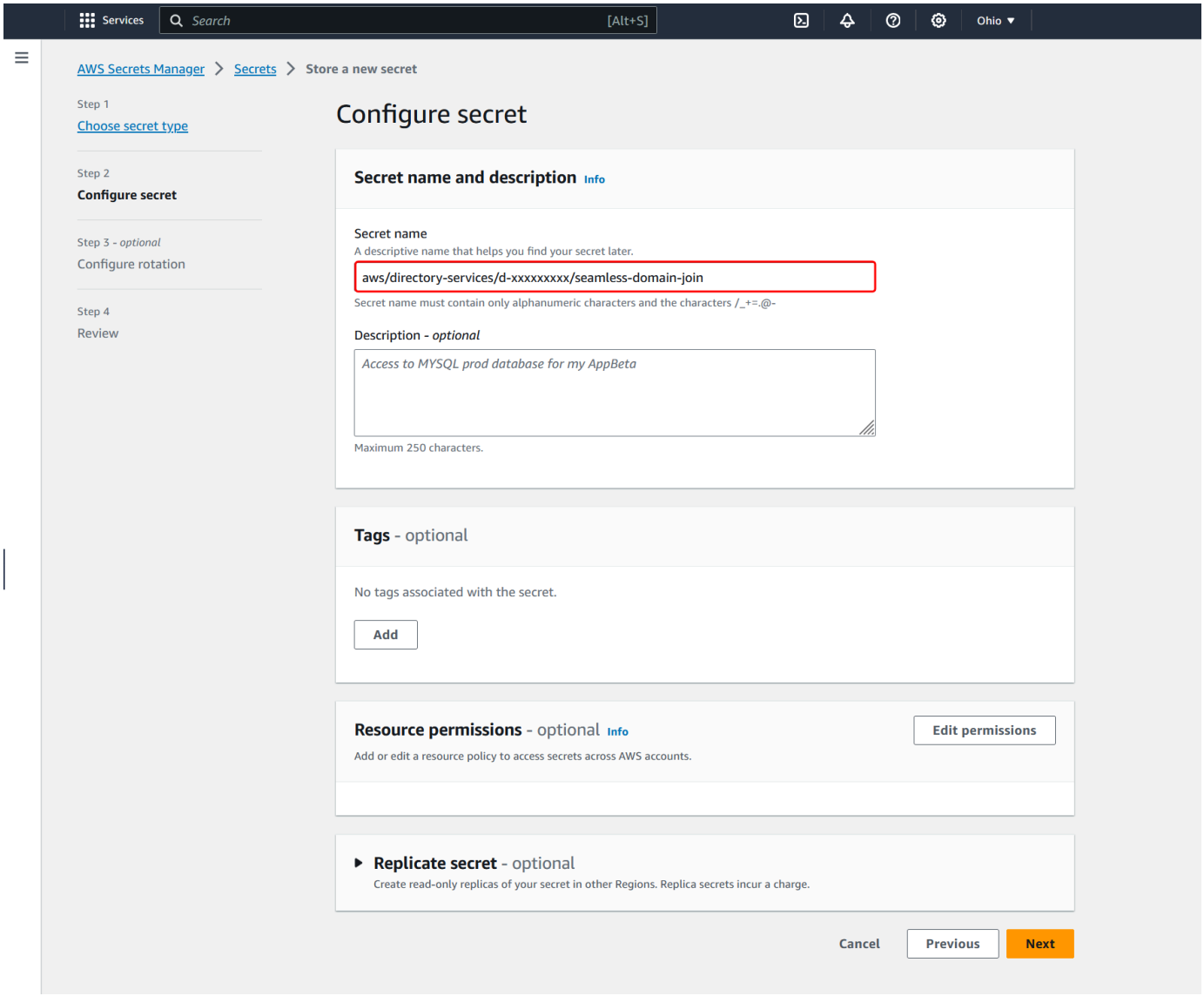
v. Pilih Berikutnya.

4. Di bawah nama Rahasia, masukkan nama rahasia yang menyertakan ID direktori Anda menggunakan format berikut, ganti *d-xxxxxxxxx* dengan ID direktori Anda:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Ini akan digunakan untuk mengambil rahasia dalam aplikasi.

> **Note**
>
> Anda harus memasukkan **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** persis seperti itu tapi ganti *d-xxxxxxxxx* dengan ID direktori Anda. Pastikan tidak ada spasi awal atau akhir. Jika tidak maka penggabungan domain akan gagal.



5. Biarkan yang lainnya diatur ke default, dan kemudian pilih Selanjutnya.
6. Di bawah Konfigurasikan rotasi otomatis, pilih Nonaktifkan rotasi otomatis, lalu pilih Selanjutnya.
7. Tinjau pengaturan, dan kemudian pilih Simpan untuk menyimpan perubahan Anda. Konsol Secrets Manager mengembalikan Anda ke daftar rahasia di akun Anda dengan rahasia baru Anda masuk di dalam daftar.
8. Pilih nama rahasia Anda yang baru dibuat dari daftar, dan perhatikan nilai ARN rahasia. Anda akan membutuhkannya di bagian selanjutnya.

Untuk membuat kebijakan dan peran IAM yang diperlukan

Gunakan langkah-langkah prasyarat berikut untuk membuat kebijakan khusus yang memungkinkan akses hanya-baca ke rahasia gabungan domain tanpa batas Secrets Manager Anda (yang Anda buat sebelumnya), dan untuk membuat peran IAM LinuxEC2 baru. DomainJoin

Membuat kebijakan membaca IAM Secrets Manager

Anda menggunakan konsol IAM untuk membuat kebijakan yang memberikan akses hanya-baca ke rahasia Secrets Manager Anda.

Untuk membuat kebijakan membaca IAM Secrets Manager

1. Masuk ke pengguna AWS Management Console sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Lalu buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, Manajemen Akses, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pilih tab JSON dan salin teks dari dokumen kebijakan JSON berikut. Kemudian tempelkan ke dalam kotak teks JSON.

> **Note**
>
> Pastikan Anda mengganti Region and Resource ARN dengan Region dan ARN sebenarnya dari rahasia yang Anda buat sebelumnya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
```

```
    ]
}
```

5. Setelah selesai, pilih Selanjutnya. Validator kebijakan melaporkan kesalahan sintaksis. Untuk informasi selengkapnya, lihat Memvalidasi kebijakan IAM.
6. Pada halaman Tinjau kebijakan, masukkan nama kebijakan, seperti **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`**. Tinjau bagian Ringkasan untuk melihat izin yang diberikan oleh kebijakan Anda. Lalu pilih Buat kebijakan untuk menyimpan perubahan Anda. Kebijakan baru muncul di daftar kebijakan terkelola dan siap dilampirkan pada identitas.

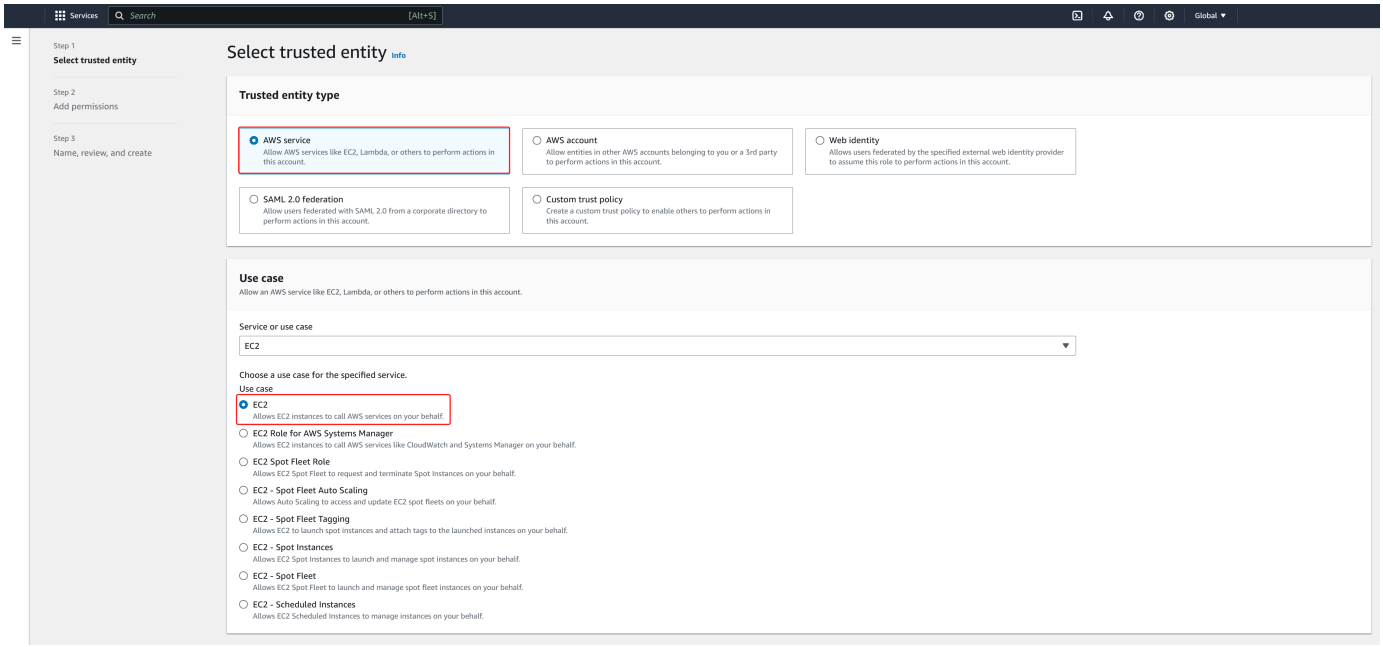
> **Note**
>
> Kami rekomendasikan Anda membuat satu kebijakan per rahasia. Melakukan hal tersebut memastikan bahwa instans hanya memiliki akses ke rahasia yang sesuai dan meminimalkan dampak jika sebuah instans dikompromikan.

Buat peran LinuXEC2 DomainJoin

Anda menggunakan konsol IAM untuk membuat peran yang akan Anda gunakan untuk penggabungan domain dengan instans EC2 Linux Anda.

Untuk membuat peran LinuXEC2 DomainJoin

1. Masuk ke pengguna AWS Management Console sebagai pengguna yang memiliki izin untuk membuat kebijakan IAM. Lalu buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, di bawah Manajemen Akses, pilih Peran.
3. Di panel konten, pilih Buat peran.
4. Di bawah Pilih jenis entitas terpercaya, pilih AWS layanan.
5. Di bawah Kasus penggunaan, pilih EC2, lalu pilih Berikutnya.



6. Untuk Kebijakan filter, lakukan hal berikut:

   a. Masukkan **`AmazonSSMManagedInstanceCore`**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   b. Masukkan **`AmazonSSMDirectoryServiceAccess`**. Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   c. Masukkan **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (atau nama kebijakan yang Anda buat dalam prosedur sebelumnya). Lalu pilih kotak centang untuk item tersebut di dalam daftar.

   d. Setelah menambahkan tiga kebijakan yang tercantum di atas, pilih Buat peran.

> **Note**
>
> AmazonSSM DirectoryServiceAccess menyediakan izin untuk menggabungkan instance ke yang dikelola oleh. Active Directory AWS Directory Service AmazonSSM ManagedInstanceCore memberikan izin minimum yang diperlukan untuk menggunakan layanan ini. AWS Systems Manager Untuk informasi selengkapnya tentang cara membuat peran dengan izin ini, dan untuk informasi tentang izin dan kebijakan lain yang dapat Anda tetapkan ke IAM role, lihat Buat profil instans IAM untuk Systems Manager di Panduan Pengguna AWS Systems Manager .

7. Masukkan nama untuk peran baru Anda, seperti **`LinuxEC2DomainJoin`** atau nama lain yang Anda inginkan di bidang Nama peran.
8. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
9. (Opsional) Pilih Tambahkan tag baru di bawah Langkah 3: Tambahkan tag untuk menambahkan tag. Pasangan nilai kunci tag digunakan untuk mengatur, melacak, atau mengontrol akses untuk peran ini.
10. Pilih Buat peran.

Bergabunglah dengan instans Linux dengan mulus ke Simple AD Active Directory Anda

Sekarang setelah Anda mengonfigurasi semua tugas prasyarat, Anda dapat menggunakan prosedur berikut untuk bergabung dengan instans Linux EC2 Anda dengan mulus.

Untuk bergabung dengan instans Linux Anda dengan mulus

1. Masuk ke AWS Management Console dan buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Dari pemilih Region di bilah navigasi, pilih yang Wilayah AWS sama dengan direktori yang ada.
3. Di Dasbor EC2, di bagian Launch instance, pilih Launch instance.
4. Pada halaman Launch an instance, di bawah bagian Name and Tags, masukkan nama yang ingin Anda gunakan untuk instans Linux EC2 Anda.
5. (Opsional) Pilih Tambahkan tag tambahan untuk menambahkan satu atau beberapa pasangan nilai kunci tag untuk mengatur, melacak, atau mengontrol akses untuk instans EC2 ini.
6. Di bagian Application and OS Image (Amazon Machine Image), pilih AMI Linux yang ingin Anda luncurkan.

> **Note**
>
> AMI yang digunakan harus memiliki AWS Systems Manager (Agen SSM) versi 2.3.1644.0 atau lebih tinggi. Untuk memeriksa versi SSM Agent yang diinstal di AMI Anda dengan meluncurkan sebuah instans dari AMI tersebut, lihat Mendapatkan versi Agen SSM yang saat ini diinstal. Jika Anda perlu meningkatkan Agen SSM, lihat Menginstal dan mengkonfigurasi SSM Agent pada instans EC2 untuk Linux.
> SSM menggunakan `aws:domainJoin` plugin saat menggabungkan instance Linux ke Active Directory domain. *`Plugin mengubah nama host untuk instance Linux ke format EC2AMAZ- XXXXXXX.`* Untuk informasi selengkapnya`aws:domainJoin`,

lihat referensi plugin dokumen AWS Systems Manager perintah di Panduan AWS Systems Manager Pengguna.

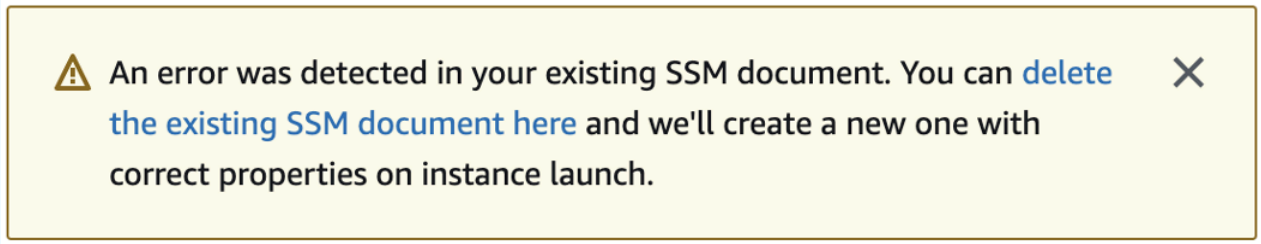
7. Di bagian Jenis instans, pilih jenis instance yang ingin Anda gunakan dari daftar dropdown tipe Instance.
8. Di bagian Key pair (login), Anda dapat memilih untuk membuat key pair baru atau memilih dari key pair yang ada. Untuk membuat key pair baru, pilih Create new key pair. Masukkan nama untuk key pair dan pilih opsi untuk Key pair type dan Private key file format. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan OpenSSH, pilih.pem. Untuk menyimpan kunci pribadi dalam format yang dapat digunakan dengan PuTTY, pilih.ppk. Pilih create key pair. File kunci privat tersebut akan secara otomatis diunduh oleh peramban Anda. Simpan file kunci privat di suatu tempat yang aman.

   ⚠ Important

   Ini adalah satu-satunya kesempatan Anda untuk menyimpan file kunci privat tersebut.
9. Pada halaman Luncurkan instance, di bawah bagian Pengaturan jaringan, pilih Edit. Pilih VPC tempat direktori Anda dibuat dari daftar dropdown yang diperlukan VPC.
10. Pilih salah satu subnet publik di VPC Anda dari daftar dropdown Subnet. Subnet yang Anda pilih harus memiliki semua lalu lintas eksternal yang diarahkan ke gateway internet. Jika hal ini tidak terjadi, Anda tidak akan dapat terhubung ke instans dari jarak jauh.

    Untuk informasi selengkapnya tentang cara menyambung ke gateway internet, lihat Connect to the internet menggunakan gateway internet di Panduan Pengguna Amazon VPC.
11. Di bawah Auto-assign IP publik, pilih Aktifkan.

    Untuk informasi selengkapnya tentang pengalamatan IP publik dan privat, lihat Pengalamatan IP instans Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Windows.
12. Untuk pengaturan Firewall (grup keamanan), Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
13. Untuk Konfigurasi pengaturan penyimpanan, Anda dapat menggunakan pengaturan default atau membuat perubahan untuk memenuhi kebutuhan Anda.
14. Pilih bagian Detail lanjutan, pilih domain Anda dari daftar dropdown direktori Gabung Domain.

> **Note**
>
> Setelah memilih direktori Gabung Domain, Anda mungkin melihat:
>
> 
>
>
> Kesalahan ini terjadi jika wizard peluncuran EC2 mengidentifikasi dokumen SSM yang ada dengan properti yang tidak terduga. Anda dapat melakukan salah satu dari yang berikut:
>
> - Jika sebelumnya Anda mengedit dokumen SSM dan properti diharapkan, pilih tutup dan lanjutkan untuk meluncurkan instans EC2 tanpa perubahan.
> - Pilih tautan hapus dokumen SSM yang ada di sini untuk menghapus dokumen SSM. Ini akan memungkinkan pembuatan dokumen SSM dengan properti yang benar. Dokumen SSM akan secara otomatis dibuat saat Anda meluncurkan instans EC2.

15. Untuk profil instans IAM, pilih peran IAM yang sebelumnya Anda buat di bagian prasyarat Langkah 2: Buat peran LinuxEC2. DomainJoin
16. Pilih Luncurkan instans.

> **Note**
>
> Jika Anda menjalankan penggabungan domain yang mulus dengan SUSE Linux, reboot diperlukan sebelum autentikasi akan bekerja. Untuk me-reboot SUSE dari terminal Linux, ketik sudo reboot.

Menggabungkan instans Amazon EC2 Linux secara manual ke Simple AD Active Directory

Selain instans Windows Amazon EC2, Anda juga dapat menggabungkan instans Amazon EC2 Linux tertentu ke Simple AD Active Directory. Distribusi instans Linux dan versi berikut ini didukung:

- Amazon Linux AMI 2018.03.0

- Amazon Linux 2 (64-bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS & Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Distribusi dan versi Linux lainnya mungkin bekerja namun belum diuji.

Prasyarat

Sebelum Anda dapat menggabungkan instans Amazon Linux, CentOS, Red Hat, atau Ubuntu ke direktori Anda, instans harus terlebih dahulu diluncurkan sebagaimana ditentukan dalam Bergabunglah dengan instans Amazon EC2 Linux dengan mulus ke Simple AD Active Directory.

> **Important**
>
> Beberapa prosedur berikut, jika tidak dilakukan dengan benar, dapat membuat instans anda tidak terjangkau atau tidak dapat digunakan. Oleh karena itu, kami sangat menyarankan Anda membuat backup atau mengambil snapshot dari instans Anda sebelum melakukan prosedur ini.

Untuk bergabung dengan instance Linux ke direktori Anda

Ikuti langkah-langkah untuk instans Linux tertentu Anda menggunakan salah satu tab berikut:

Amazon Linux

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya

di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Amazon Linux - 64bit Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Amazon Linux yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Untuk bantuan dalam menentukan versi Amazon Linux yang Anda gunakan, lihat Mengidentifikasi image Amazon Linux dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Akun pada domain *example.com* yang memiliki hak istimewa untuk penggabungan domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.
   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

7. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:
   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

CentOS

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans CentOS 7 Anda adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket CentOS 7 yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Akun pada domain *example.com* yang memiliki hak istimewa untuk penggabungan domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

7. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

Red hat

1. Terhubung ke instans menggunakan klien SSH apa saja.

2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.
3. Pastikan instans Red Hat - 64bit adalah yang terbaru.

```
sudo yum -y update
```

4. Instal paket Red Hat yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

SAM AccountName untuk akun di domain *example.com* yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

6. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.

   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

7. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:

   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan “\<space>" untuk membuat karakter spasi Linux.)

Ubuntu

1. Terhubung ke instans menggunakan klien SSH apa saja.
2. Konfigurasikan instance Linux untuk menggunakan alamat IP server DNS dari server DNS AWS Directory Service yang disediakan. Anda dapat melakukan ini baik dengan mengaturnya di set Opsi DHCP yang terlampir pada VPC atau dengan mengaturnya secara manual pada

instans. Jika Anda ingin mengaturnya secara manual, lihat Bagaimana cara menetapkan server DNS statis ke instans Amazon EC2 privat dalam Pusat Pengetahuan AWS untuk pedoman tentang pengaturan server DNS persisten untuk distribusi dan versi Linux tertentu Anda.

3. Pastikan instans Ubuntu - 64bit Anda adalah yang terbaru.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Instal paket Ubuntu yang diperlukan pada instans Linux Anda.

> **Note**
>
> Beberapa paket ini mungkin sudah diinstal.
> Ketika Anda menginstal paket, Anda mungkin akan disajikan dengan beberapa layar konfigurasi pop-up. Anda biasanya dapat membiarkan bidang di layar ini kosong.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Nonaktifkan resolusi Reverse DNS dan atur ranah default ke FQDN domain Anda. Instans Ubuntu harus dapat dipecahkan terbalik di DNS sebelum ranah akan bekerja. Jika tidak, Anda harus menonaktifkan DNS terbalik di /etc/krb5.conf sebagai berikut:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Menggabungkan instans ke direktori dengan perintah berikut.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

SAM AccountName untuk akun di domain *example.com* yang memiliki hak istimewa bergabung domain. Masukkan kata sandi untuk akun saat diminta. Untuk informasi

selengkapnya tentang mendelegasikan hak istimewa ini, lihat Mendelegasikan hak istimewa penggabungan direktori untuk Microsoft AD yang Dikelola AWS.

example.com

Nama DNS yang memenuhi syarat untuk direktori Anda.

```
...
 * Successfully enrolled machine in realm
```

7. Mengatur layanan SSH untuk mengizinkan autentikasi kata sandi.
   a. Buka file `/etc/ssh/sshd_config` di editor teks.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Atur pengaturan `PasswordAuthentication` ke `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Mulai ulang layanan SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   Atau:

   ```
   sudo service sshd restart
   ```

8. Setelah instans telah dimulai ulang, hubungkan dengan klien SSH mana pun dan tambahkan grup admin domain ke daftar sudoers dengan melakukan langkah-langkah berikut:
   a. Buka file `sudoers` dengan perintah berikut:

   ```
   sudo visudo
   ```

   b. Tambahkan hal berikut ini ke bagian bawah file `sudoers` dan simpan.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Contoh di atas menggunakan "\<space>" untuk membuat karakter spasi Linux.)

> **Note**
>
> Saat menggunakan Simple AD, jika Anda membuat akun pengguna pada instans Linux dengan opsi “Paksa pengguna untuk mengubah kata sandi saat login pertama,” pengguna tersebut tidak akan dapat mengubah kata sandi mereka menggunakan kpasswd. Untuk mengubah kata sandi pertama kalinya, administrator domain harus memperbarui sandi pengguna menggunakan Alat Pengelolaan Direktori Aktif.

Mengelola akun dari instans Linux

Untuk mengelola akun di Simple AD dari instans Linux, Anda harus memperbarui file konfigurasi tertentu pada instans Linux Anda sebagai berikut:

1. Atur krb5_use_kdcinfo ke Salah di file /etc/sssd/sssd.conf. Sebagai contoh:

   ```
   [domain/example.com]
       krb5_use_kdcinfo = False
   ```

2. Agar konfigurasi mulai berlaku Anda perlu memulai ulang layanan sssd:

   ```
   $ sudo systemctl restart sssd.service
   ```

   Atau, Anda dapat menggunakan .

   ```
   $ sudo service sssd start
   ```

3. Jika Anda akan mengelola pengguna dari instans CentOS Linux, Anda juga harus mengedit file / etc/smb.conf untuk memasukkan:

   ```
   [global]
     workgroup = EXAMPLE.COM
     realm = EXAMPLE.COM
     netbios name = EXAMPLE
     security = ads
   ```

Membatasi akses login akun

Karena semua akun ditetapkan dalam Direktori Aktif, secara default, semua pengguna dalam direktori tersebut dapat masuk ke instans. Anda dapat mengizinkan hanya pengguna tertentu untuk masuk ke instans dengan ad_access_filter di sssd.conf. Sebagai contoh:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Menunjukkan bahwa pengguna hanya boleh diizinkan akses ke instans jika mereka adalah anggota dari grup tertentu.

cn

Nama umum grup yang harus memiliki akses. Dalam contoh ini, nama grupnya adalah *admins*.

ou

Ini adalah unit organisasi tempat grup di atas berada. Dalam contoh ini, OU adalah *Testou*.

dc

Ini adalah komponen domain dari domain Anda. Dalam contoh ini, *example*.

dc

Ini adalah komponen domain tambahan. Dalam contoh ini, *com*.

Anda harus menambahkan ad_access_filter secara manual ke /etc/sssd/sssd.conf.

Buka file /etc/sssd/sssd.conf di editor teks.

```
sudo vi /etc/sssd/sssd.conf
```

Setelah melakukan hal ini, sssd.conf Anda mungkin terlihat seperti ini:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
```

```
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Agar konfigurasi mulai berlaku, Anda perlu memulai ulang layanan sssd:

```
sudo systemctl restart sssd.service
```

Atau, Anda dapat menggunakan .

```
sudo service sssd restart
```

Pemetaan ID

Pemetaan ID dapat dilakukan dengan dua metode untuk mempertahankan pengalaman terpadu antara identitas UNIX/Linux User Identifier (UID) dan Group Identifier (GID) dan Windows and Security Identifier (SID). Active Directory

1. Terpusat
2. Didistribusikan

> **Note**
>
> Pemetaan identitas pengguna terpusat di Active Directory memerlukan Antarmuka Sistem Operasi Portabel atau POSIX.

Pemetaan identitas pengguna terpusat

Active Directoryatau layanan Lightweight Directory Access Protocol (LDAP) lainnya menyediakan UID dan GID kepada pengguna Linux. DalamActive Directory, pengidentifikasi ini disimpan dalam atribut pengguna:

- UID - Nama pengguna Linux (String)
- Nomor UID - Nomor ID Pengguna Linux (Integer)
- Nomor GID - Nomor ID Grup Linux (Integer)

Untuk mengkonfigurasi instance Linux untuk menggunakan UID dan GID dariActive Directory, atur `ldap_id_mapping = False` dalam file sssd.conf. Sebelum menyetel nilai ini, verifikasi bahwa Anda telah menambahkan UID, nomor UID, dan nomor GID ke pengguna dan grup. Active Directory

Pemetaan identitas pengguna terdistribusi

Jika Active Directory tidak memiliki ekstensi POSIX atau jika Anda memilih untuk tidak mengelola pemetaan identitas secara terpusat, Linux dapat menghitung nilai UID dan GID. Linux menggunakan Security Identifier (SID) unik pengguna untuk menjaga konsistensi.

Untuk mengonfigurasi pemetaan ID pengguna terdistribusi, atur `ldap_id_mapping = True` dalam file sssd.conf.

Connect ke instance Linux

Ketika pengguna terhubung ke instance menggunakan klien SSH, mereka diminta untuk nama pengguna mereka. Pengguna dapat memasukkan nama pengguna dalam `EXAMPLE\username` format `username@example.com` atau. Respons akan muncul mirip dengan yang berikut ini, tergantung pada distribusi Linux yang Anda gunakan:

Amazon Linux, Red Hat Enterprise Linux, dan CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Mendelegasikan hak istimewa penggabungan direktori untuk Simple AD

Untuk bergabung dengan komputer ke direktori Anda, Anda memerlukan akun yang memiliki hak istimewa untuk menggabungkan komputer ke direktori.

Dengan Simple AD, anggota grup Admin domain memiliki hak istimewa yang memadai untuk menggabungkan komputer ke direktori.

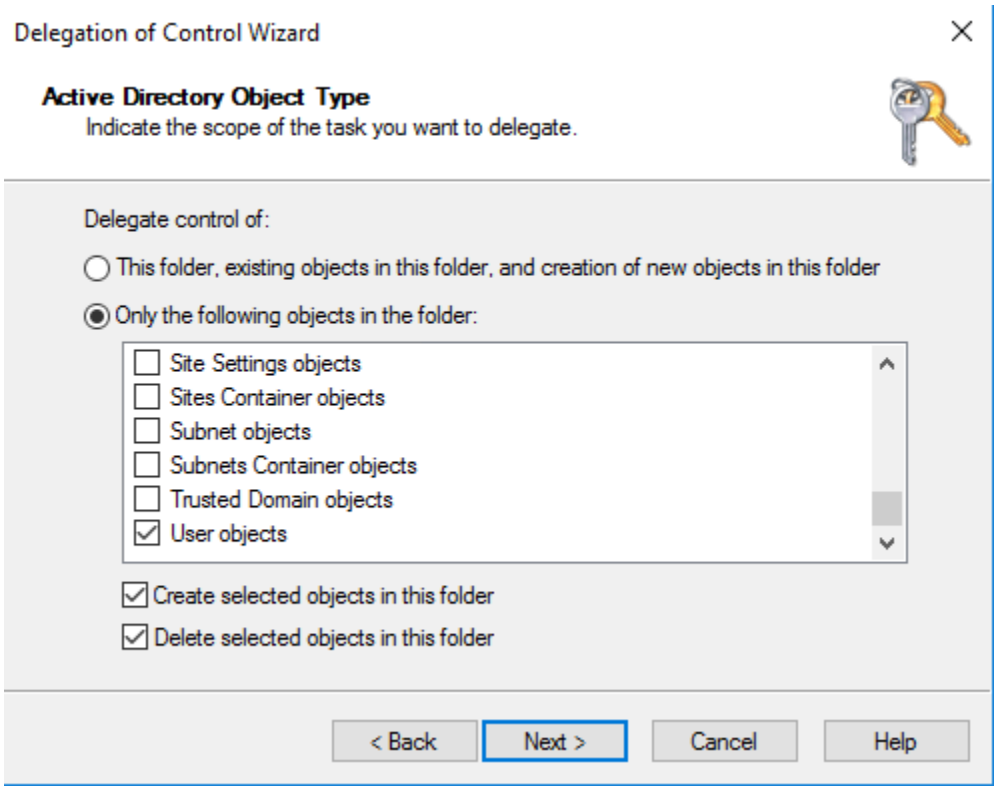
Namun, sebagai praktik terbaik, Anda harus menggunakan akun yang hanya memiliki hak istimewa minimum yang diperlukan. Prosedur berikut menunjukkan cara membuat grup baru yang disebut `Joiners` dan mendelegasikan hak istimewa untuk grup ini yang diperlukan untuk menggabungkan komputer ke direktori.

Anda harus melakukan prosedur ini pada komputer yang telah tergabung ke direktori Anda dan memiliki MMC snap-in Pengguna dan Komputer Direktori Aktif terinstal. Anda juga harus masuk sebagai administrator domain.

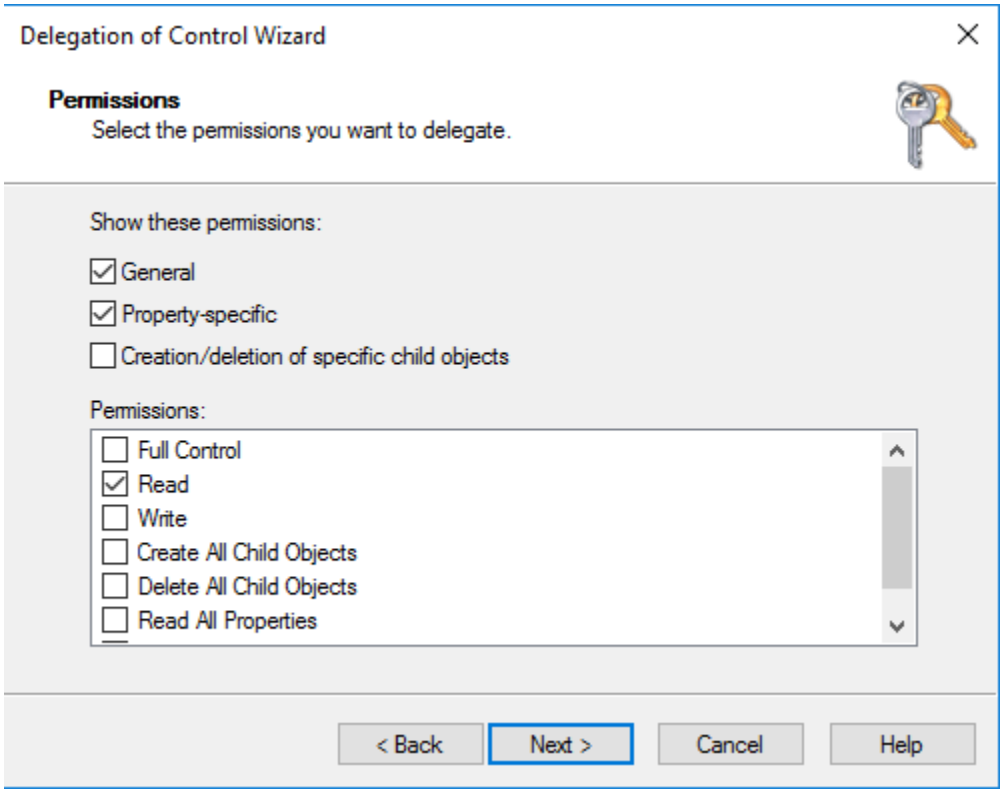
Untuk mendelegasikan hak istimewa penggabungan direktori untuk Simple AD

1. Buka Pengguna dan Komputer Direktori Aktif dan pilih root domain Anda di pohon navigasi.

2. Di pohon navigasi sebelah kiri, buka menu konteks (klik kanan) untuk Pengguna, pilih Baru, lalu pilih Grup.
3. Di kotak Objek Baru - Grup, ketik hal berikut dan pilih OK.
   - Untuk Nama grup, ketik **`Joiners`**.
   - Untuk Cakupan grup, pilih Global.
   - Untuk Jenis grup, pilih Keamanan.
4. Pada pohon navigasi, pilih root domain Anda. Dari menu Tindakan, pilih Kendali Delegasi.
5. Pada halaman Delegasi Control Wizard, pilih Selanjutnya, lalu pilih Tambahkan.
6. Di kotak Pilih Pengguna, Komputer, atau Grup, ketik `Joiners` dan pilih OK. Jika ditemukan lebih dari satu objek, pilih grup `Joiners` yang dibuat di atas. Pilih Berikutnya.
7. Pada halaman Tugas untuk Didelegasikan, pilih Buat tugas kustom untuk didelegasikan, lalu pilih Selanjutnya.
8. Pilih Hanya objek berikut dalam folder, lalu pilih Objek komputer.
9. Pilih Buat objek yang dipilih dalam folder ini dan Hapus objek yang dipilih dalam folder ini. Lalu pilih Selanjutnya.



10. Pilih Baca dan Tulis, lalu pilih Selanjutnya.



11. Verifikasi informasi pada halaman Menyelesaikan Delegasi Control Wizard, dan klik Selesai.
12. Buat pengguna dengan kata sandi yang kuat dan tambahkan pengguna tersebut ke grup `Joiners`. Pengguna kemudian akan memiliki hak istimewa yang cukup untuk terhubung AWS Directory Service ke direktori.

Buat set opsi DHCP

AWS merekomendasikan agar Anda membuat set opsi DHCP untuk AWS Directory Service direktori Anda dan menetapkan opsi DHCP yang disetel ke VPC tempat direktori Anda berada. Ini memungkinkan setiap instans di VPC tersebut mengarah ke domain tertentu, dan server DNS untuk menyelesaikan nama domain mereka.

Untuk informasi selengkapnya tentang set opsi DHCP, lihat Set opsi DHCP di Panduan Pengguna Amazon VPC.

Untuk membuat set opsi DHCP untuk direktori Anda

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di panel navigasi, pilih Set Opsi DHCP, lalu pilih Buat set opsi DHCP.
3. Pada halaman Buat set opsi DHCP, masukkan nilai berikut untuk direktori Anda:

Nama

Tanda opsional untuk set opsi.

Nama domain

Nama yang memenuhi syarat untuk direktori, seperti `corp.example.com`.

Server nama domain

Alamat IP server DNS direktori AWS-provided Anda.

> **Note**
>
> Anda dapat menemukan alamat ini dengan membuka panel navigasi Konsol AWS Directory Service, memilih direktori dan kemudian memilih ID direktori yang benar.

Server NTP

Biarkan bidang ini kosong.

Server nama NetBIOS

Biarkan bidang ini kosong.

Jenis simpul NetBIOS

Biarkan bidang ini kosong.

4. Pilih Buat set opsi DHCP. Set opsi DHCP baru muncul dalam daftar opsi DHCP Anda.
5. Catat ID dari set opsi DHCP yang baru (dopt-*xxxxxxxx*). Anda menggunakannya untuk mengasosiasikan set opsi yang baru dengan VPC Anda.

Untuk mengubah set opsi DHCP yang terkait dengan VPC

Setelah Anda membuat set opsi DHCP, Anda tidak dapat mengubahnya. Jika Anda ingin VPC Anda untuk menggunakan set opsi DHCP yang berbeda, Anda harus membuat satu set baru dan mengasosiasikannya dengan VPC Anda. Anda juga dapat mengatur VPC Anda untuk tidak menggunakan opsi DHCP sama sekali.

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.

2. Di panel navigasi, pilih VPC Anda
3. Pilih VPC, lalu pilih Tindakan, Edit set opsi DHCP.
4. Untuk Set opsi DHCP, pilih satu set opsi atau pilih Tidak ada set opsi DHCP, lalu pilih Simpan.

Memelihara direktori Simple AD

Bagian ini menjelaskan cara memelihara tugas administratif umum untuk lingkungan Simple AD Anda.

Topik

- Hapus Simple AD Anda
- Snapshot atau pulihkan direktori Anda
- Melihat informasi direktori

Hapus Simple AD Anda

Ketika Simple AD dihapus, semua data direktori dan snapshot dihapus dan tidak dapat dipulihkan. Setelah direktori dihapus, semua instans yang bergabung ke direktori tetap utuh. Anda tidak dapat, bagaimanapun, menggunakan kredensial direktori Anda untuk masuk ke instans ini. Anda harus log in ke instans ini dengan akun pengguna yang lokal untuk instans.

Untuk menghapus direktori

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori. Pastikan Anda berada di Wilayah AWS tempat Anda Active Directory dikerahkan. Untuk informasi selengkapnya, lihat Memilih Wilayah.
2. Pastikan tidak ada AWS aplikasi yang diaktifkan untuk direktori yang ingin Anda hapus. AWS Aplikasi yang diaktifkan akan mencegah Anda menghapus iklan Microsoft AWS Terkelola atau Simple AD Anda.

    a. Pada halaman Direktori, pilih ID direktori Anda.

    b. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi. Di bagian AWS aplikasi & layanan, Anda melihat AWS aplikasi mana yang diaktifkan untuk direktori Anda.

        - Nonaktifkan AWS Management Console akses.

- Untuk menonaktifkan Amazon WorkSpaces, Anda harus membatalkan pendaftaran layanan dari direktori di konsol. WorkSpaces Untuk informasi selengkapnya, lihat membatalkan pendaftaran dari direktori di Panduan Administrasi Amazon WorkSpaces .
- Untuk menonaktifkan Amazon WorkDocs, Anda harus menghapus WorkDocs situs Amazon di WorkDocs konsol Amazon. Untuk informasi selengkapnya, lihat Menghapus situs di Panduan WorkDocs Administrasi Amazon.
- Untuk menonaktifkan Amazon WorkMail, Anda harus menghapus WorkMail organisasi Amazon di WorkMail konsol Amazon. Untuk informasi selengkapnya, lihat Menghapus organisasi di Panduan WorkMail Administrator Amazon.
- Untuk menonaktifkan Amazon FSx for Windows File Server, Anda harus menghapus sistem file Amazon FSx dari domain. Untuk informasi selengkapnya, lihat Bekerja dengan Active Directory di FSx for Windows File Server di Panduan Pengguna Amazon FSx for Windows File Server.
- Untuk menonaktifkan Amazon Relational Database Service, Anda harus menghapus instans Amazon RDS dari domain. Untuk informasi selengkapnya, lihat Mengelola instans DB dalam domain dalam Panduan Pengguna Amazon RDS.
- Untuk menonaktifkan AWS Client VPN Layanan, Anda harus menghapus layanan direktori dari Endpoint Client VPN. Untuk informasi selengkapnya, lihat Active DirectoryOtentikasi di Panduan AWS Client VPN Administrator.
- Untuk menonaktifkan Amazon Connect, Anda harus menghapus Instans Amazon Connect. Untuk informasi selengkapnya, lihat Menghapus instans Amazon Connect dalam Panduan Administrator Amazon Connect.
- Untuk menonaktifkan Amazon QuickSight, Anda harus berhenti berlangganan dari Amazon QuickSight. Untuk informasi selengkapnya, lihat Menutup Amazon QuickSight akun Anda di Panduan QuickSight Pengguna Amazon.

> **Note**
>
> Jika Anda menggunakan AWS IAM Identity Center dan sebelumnya telah menghubungkannya ke direktori Microsoft AD AWS Terkelola yang ingin Anda hapus, Anda harus terlebih dahulu mengubah sumber identitas sebelum dapat menghapusnya. Untuk informasi selengkapnya, lihat Mengubah sumber identitas Anda di Panduan Pengguna Pusat Identitas IAM.

3. Di panel navigasi, pilih Direktori.

4. Pilih hanya direktori yang akan dihapus dan klik Hapus. Ini akan memerlukan beberapa menit agar direktori dihapus. Ketika direktori telah dihapus, itu akan dihapus dari daftar direktori Anda.

Snapshot atau pulihkan direktori Anda

AWS Directory Service menyediakan kemampuan untuk mengambil snapshot manual dari data untuk direktori Simple AD Anda. Snapshot ini dapat digunakan untuk melakukan point-in-time pemulihan untuk direktori Anda. Anda tidak dapat mengambil snapshot dari direktori AD Connector.

Topik

Membuat snapshot dari direktori Anda

Snapshot dapat digunakan untuk memulihkan direktori Anda ke apa itu pada titik waktu yang snapshot diambil. Untuk membuat snapshot manual dari direktori Anda, lakukan langkah-langkah berikut.

> **Note**
>
> Anda dibatasi hingga 5 snapshot manual untuk setiap direktori. Jika Anda telah mencapai batas ini, Anda harus menghapus salah satu snapshot manual yang ada sebelum Anda dapat membuat yang lain.

Untuk membuat snapshot manual

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Membuat snapshot.
5. Pada kotak dialog Membuat snapshot direktori, berikan nama untuk snapshot, jika diinginkan. Ketika siap, pilih Buat.

Tergantung pada ukuran direktori Anda, mungkin diperlukan beberapa menit untuk membuat snapshot. Ketika snapshot siap, nilai Status akan berubah menjadi `Completed`.

Memulihkan direktori Anda dari snapshot

Memulihkan direktori dari snapshot setara dengan memindahkan direktori kembali ke waktu dulu. Direktori snapshot unik untuk direktori tempat mereka dibuat. Snapshot hanya dapat dipulihkan ke direktori dari mana ia dibuat. Selain itu, usia maksimum yang didukung dari snapshot manual adalah 180 hari. Untuk informasi selengkapnya, lihat Masa simpan yang berguna dari backup keadaan sistem Direktori Aktif di situs web Microsoft.

> **Warning**
>
> Kami rekomendasikan Anda menghubungi Pusat AWS Support sebelum pemulihan snapshot apa pun; kami mungkin dapat membantu Anda menghindari kebutuhan untuk melakukan pemulihan snapshot. Setiap pemulihan dari snapshot dapat mengakibatkan kehilangan data karena mereka adalah titik waktu. Penting untuk Anda memahami bahwa semua server DC dan DNS yang terasosiasi dengan direktori akan offline sampai operasi pemulihan telah selesai.

Untuk memulihkan direktori Anda dari snapshot, lakukan langkah-langkah berikut.

Untuk memulihkan direktori dari snapshot

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih snapshot dalam daftar, pilih Tindakan, dan kemudian pilih Memulihkan snapshot.
5. Tinjau informasi di kotak dialog Memulihkan snapshot direktori, dan pilih Pemulihan.

Untuk direktori, mungkin diperlukan beberapa menit untuk direktori dipulihkan. Ketika berhasil dipulihkan, nilai Status direktori berubah menjadi `Active`. Setiap perubahan yang dibuat ke direktori setelah tanggal snapshot akan ditimpa.

Menghapus snapshot

Untuk menghapus snapshot

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pemeliharaan.
4. Di bagian Snapshot, pilih Tindakan, dan kemudian pilih Hapus snapshot.
5. Verifikasi bahwa Anda ingin menghapus snapshot tersebut, lalu pilih Hapus.

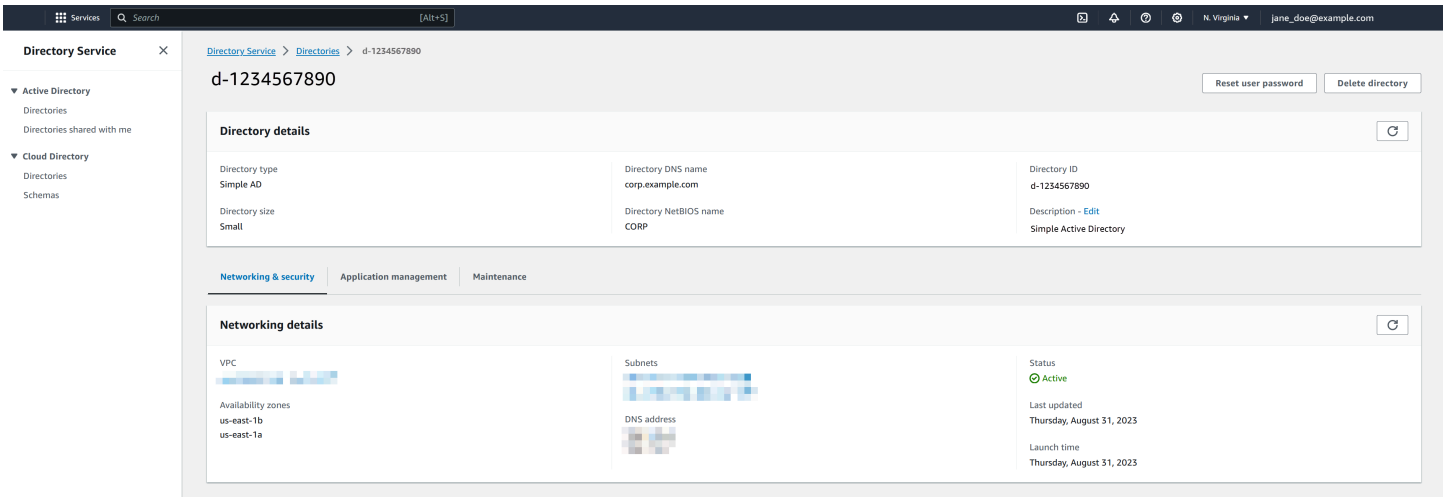
Melihat informasi direktori

Anda dapat melihat informasi detail tentang direktori.

Untuk melihat informasi direktori terperinci.

1. Di panel navigasi AWS Directory Service konsol, di bawah Active Directory, pilih Direktori.
2. Klik tautan ID direktori untuk direktori Anda. Informasi tentang direktori ditampilkan dalam halaman Detail direktori.

Untuk informasi selengkapnya tentang bidang Status, lihat Memahami status direktori Anda.



Aktifkan akses ke AWS aplikasi dan layanan

Pengguna dapat mengotorisasi Simple AD untuk memberikan AWS aplikasi dan layanan, seperti Amazon WorkSpaces, akses ke aplikasi AndaActive Directory. AWS Aplikasi dan layanan berikut dapat diaktifkan atau dinonaktifkan untuk bekerja dengan Simple AD.

AWS aplikasi/layanan	Informasi selengkapnya…
Amazon Chime	Untuk informasi selengkapnya, lihat Panduan Administrasi Amazon Chime.
Amazon WorkDocs	Untuk informasi selengkapnya, lihat Panduan WorkDocs Administrasi Amazon
Amazon WorkMail	Untuk informasi selengkapnya, lihat Panduan WorkMail Administrator Amazon.
Amazon WorkSpaces	Anda dapat membuat Simple AD, AWS Managed Microsoft AD, atau AD Connector langsung dari WorkSpaces. Cukup luncurkan Pengaturan Advanced saat membuat Workspace Anda. Untuk informasi selengkapnya, lihat Panduan WorkSpaces Administrasi Amazon.
AWS Management Console	Untuk informasi selengkapnya, lihat Mengaktifkan akses ke AWS Management Console dengan kredensial AD.

Setelah diaktifkan, Anda mengelola akses ke direktori Anda di konsol dari aplikasi atau layanan yang ingin Anda berikan akses ke direktori Anda. Untuk menemukan tautan AWS aplikasi dan layanan yang dijelaskan di atas di AWS Directory Service konsol, lakukan langkah-langkah berikut.

Untuk menampilkan aplikasi dan layanan untuk direktori

1. Pada panel navigasi konsolAWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.

3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Tinjau daftar di bawah bagian aplikasi & layananAWS .

Untuk informasi selengkapnya tentang cara mengotorisasi atau membatalkan otorisasi AWS aplikasi dan layanan yang digunakan AWS Directory Service, lihat. Otorisasi untuk AWS aplikasi dan layanan menggunakan AWS Directory Service

Topik

- Membuat URL akses
- Sign-on tunggal

Membuat URL akses

URL akses digunakan dengan aplikasi dan layanan AWS, seperti Amazon WorkDocs, untuk mencapai halaman login yang terasosiasi dengan direktori Anda. URL harus unik secara global. Anda dapat membuat URL akses untuk direktori Anda dengan melakukan langkah-langkah berikut.

> **Warning**
>
> Setelah Anda membuat URL akses aplikasi untuk direktori ini, itu tidak dapat diubah. Setelah URL akses dibuat, tidak dapat digunakan oleh orang lain. Jika Anda menghapus direktori Anda, URL akses juga dihapus dan kemudian dapat digunakan oleh akun lain.

Untuk membuat URL akses

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bagian URL akses aplikasi, jika URL akses belum ditetapkan ke direktori, tombol Buat ditampilkan. Masukkan alias direktori dan pilih Buat. Jika error Entitas Sudah Ada dikembalikan, alias direktori tertentu telah dialokasikan. Pilih alias lain dan ulangi prosedur ini.

   URL akses Anda ditampilkan dalam format *<alias>*.awsapps.com.

Sign-on tunggal

AWS Directory Servicemenyediakan kemampuan untuk memungkinkan pengguna Anda mengakses Amazon WorkDocs dari komputer yang bergabung ke direktori tanpa harus memasukkan kredensialnya secara terpisah.

Sebelum mengaktifkan sing-on tunggal, Anda perlu mengambil langkah tambahan agar peramban web pengguna dapat mendukung sign-on tunggal. Pengguna mungkin perlu memodifikasi pengaturan peramban web mereka untuk mengaktifkan sign-on tunggal.

> **Note**
>
> Sign-on tunggal hanya bekerja bila digunakan pada komputer yang digabungkan ke direktori AWS Directory Service. Ini tidak dapat digunakan pada komputer yang tidak bergabung ke direktori.

Jika direktori Anda adalah direktori AD Connector dan akun layanan AD Connector tidak memiliki izin untuk menambahkan atau menghapus atribut nama utama layanannya, maka untuk Langkah 5 dan 6 di bawah ini, Anda memiliki dua pilihan:

1. Anda dapat melanjutkan dan akan diminta untuk nama pengguna dan kata sandi untuk pengguna direktori yang memiliki izin ini untuk menambah atau menghapus atribut nama utama layanan pada akun layanan AD Connector. Kredensial ini hanya digunakan untuk mengaktifkan sign-on tunggal dan tidak disimpan oleh layanan. Izin akun layanan AD Connector tidak berubah.
2. Anda dapat mendelegasikan izin untuk mengizinkan akun layanan AD Connector menambah atau menghapus atribut nama utama layanan itu sendiri, Anda dapat menjalankan PowerShell perintah di bawah ini dari komputer yang bergabung dengan domain menggunakan akun yang memiliki izin untuk mengubah izin pada akun layanan AD Connector. Perintah di bawah ini akan memberikan akun layanan AD Connector kemampuan untuk menambah dan menghapus atribut nama utama layanan hanya untuk dirinya sendiri.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
```

```
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Untuk mengaktifkan atau menonaktifkan sistem masuk tunggal dengan Amazon WorkDocs

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bagian URL akses aplikasi, pilih Aktifkan untuk mengaktifkan sistem masuk tunggal untuk Amazon. WorkDocs

   Jika Anda tidak melihat tombol Aktifkan, Anda mungkin harus terlebih dahulu membuat URL Akses sebelum opsi ini akan ditampilkan. Untuk informasi selengkapnya tentang cara membuat URL akses, lihat Membuat URL akses.
5. Di kotak dialog Aktifkan Sign-On Tunggal untuk direktori ini,, pilih Aktifkan. Sign-on tunggal diaktifkan untuk direktori.
6. Jika nanti Anda ingin menonaktifkan sistem masuk tunggal dengan Amazon WorkDocs, pilih Nonaktifkan, lalu di kotak dialog Nonaktifkan Single Sign-On untuk direktori ini, pilih Nonaktifkan lagi.

Topik

- Sign-on tunggal untuk IE dan Chrome
- Sign-on tunggal untuk Firefox

Sign-on tunggal untuk IE dan Chrome

Untuk mengizinkan peramban Microsoft Internet Explorer (IE) dan Google Chrome untuk mendukung sign-on tunggal, tugas berikut harus dilakukan pada komputer klien:

- Tambahkan URL akses Anda (misalnya, https://*<alias>*.awsapps.com) ke daftar situs yang disetujui untuk sign-on tunggal.
- Aktifkan skrip aktif (JavaScript).
- Izinkan masuk otomatis.
- Aktifkan autentikasi terintegrasi.

Anda atau pengguna Anda dapat melakukan tugas-tugas ini secara manual, atau Anda dapat mengubah pengaturan ini menggunakan pengaturan Kebijakan Grup.

Topik

- Pembaruan manual untuk sign-on tunggal pada Windows
- Pembaruan manual untuk sign-on tunggal pada OS X
- Pengaturan kebijakan grup untuk sign-on tunggal

Pembaruan manual untuk sign-on tunggal pada Windows

Untuk mengaktifkan sign-on tunggal secara manual pada komputer Windows, lakukan langkah-langkah berikut pada komputer klien. Beberapa pengaturan ini mungkin sudah diatur dengan benar.

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome secara manual di Windows

1. Untuk membuka kotak dialog Properti internet, pilih menu Start, ketik `Internet Options` di kotak pencarian, lalu pilih Opsi Internet.
2. Tambahkan URL akses Anda ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
    a. Di kotak dialog Properti internet, pilih tab Keamanan.
    b. Pilih Intranet lokal dan pilih Situs.
    c. Di kotak dialog Intranet lokal, pilih Advanced.
    d. Tambahkan URL akses Anda ke daftar situs web dan pilih tutup.
    e. Di dialog box Intranet lokal, pilih OK.

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:

   a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.

   b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Penulisan dan pilih Aktifkan di bawah Penulisan aktif.

   c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.

4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:

   a. Di tab Keamanan dari kotak dialog Properti internet, pilih Tingkat kustom.

   b. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, gulir ke bawah untuk Autentikasi Pengguna dan pilih Masuk otomatis hanya di zona Intranet di bawah Masuk.

   c. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.

   d. Di kotak dialog Pengaturan Keamanan - Zona Intranet Lokal, pilih OK.

5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:

   a. Di kotak dialog Properti internet, pilih tab Advanced.

   b. Gulir ke bawah ke Keamanan dan pilih Mengaktifkan Autentikasi Windows Terintegrasi.

   c. Di kotak dialog Properti Internet, pilih OK.

6. Tutup dan buka kembali peramban Anda agar perubahan ini berlaku.

Pembaruan manual untuk sign-on tunggal pada OS X

Untuk mengaktifkan sign-on tunggal secara manual untuk Chrome pada OS X, lakukan langkah-langkah berikut pada komputer klien. Anda memerlukan hak administrator di komputer Anda untuk menyelesaikan langkah-langkah ini.

Cara mengaktifkan sign-on tunggal untuk Chrome di OS X secara manual

1. Tambahkan URL akses Anda ke AuthServerAllowlistkebijakan dengan menjalankan perintah berikut:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Buka Preferensi Sistem, buka panel Profil, dan hapus profil `Chrome Kerberos Configuration`.
3. Mulai ulang Chrome dan buka chrome://policy di Chrome untuk mengonfirmasi bahwa pengaturan baru sudah terpasang.

Pengaturan kebijakan grup untuk sign-on tunggal

Administrator domain dapat menerapkan pengaturan Kebijakan Grup untuk membuat perubahan sign-on tunggal pada komputer klien yang digabungkan ke domain.

> **Note**
>
> Jika Anda mengelola browser web Chrome di komputer di domain Anda dengan kebijakan Chrome, Anda harus menambahkan URL akses ke AuthServerAllowlistkebijakan. Untuk informasi selengkapnya tentang mengatur kebijakan Chrome, kunjungi Pengaturan Kebijakan di Chrome.

Cara mengaktifkan sign-on tunggal untuk Internet Explorer dan Chrome menggunakan pengaturan Kebijakan Grup

1. Membuat objek Kebijakan Grup baru dengan melakukan langkah-langkah berikut:
   a. Buka alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, lalu pilih Objek Kebijakan Grup.
   b. Dari menu utama, pilih Tindakan dan pilih Baru.
   c. Di kotak dialog GPO baru, masukkan nama deskriptif untuk objek Kebijakan Grup, seperti `IAM Identity Center Policy`, dan biarkan Sumber Starter GPO diatur ke (tidak ada). Klik OK.
2. Tambahkan URL akses ke daftar situs yang disetujui untuk sign-on tunggal dengan melakukan langkah-langkah berikut:
   a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.
   b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.
   c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.

d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

   Aksi

   ```
   Update
   ```

   Sarang

   ```
   HKEY_CURRENT_USER
   ```

   Jalan

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   \ZoneMap\Domains\awsapps.com\<alias>
   ```

   Nilai untuk *<alias>* berasal dari URL akses Anda. Jika URL akses Anda adalah `https://examplecorp.awsapps.com`, alias adalah `examplecorp`, dan kunci registri akan menjadi `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

   Nama nilai

   ```
   https
   ```

   Jenis nilai

   ```
   REG_DWORD
   ```

   Data nilai

   ```
   1
   ```

3. Untuk mengaktifkan penulisan aktif, lakukan langkah-langkah berikut ini:

   a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.

   b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.

   c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Izinkan penulisan aktif dan pilih Edit.

   d. Di kotak dialog Izinkan penulisan aktif, masukkan pengaturan berikut dan pilih OK:

      - Pilih tombol radio Diaktifkan.

- Di bawah Opsi atur Izinkan penulisan aktif ke Aktifkan.

4. Untuk mengaktifkan masuk otomatis, lakukan langkah-langkah berikut ini:

   a. Pada alat Pengelolaan Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan SSO Anda, lalu pilih Edit.

   b. Di pohon kebijakan, arahkan ke Konfigurasi komputer > Kebijakan > Templat Administrasi > Komponen Windows > Internet Explorer > Panel Kontrol Internet > Halaman Keamanan > Zona Intranet.

   c. Di daftar Zona Intranet, buka menu konteks (klik kanan) untuk Opsi masuk dan pilih Edit.

   d. Di kotak dialog Opsi masuk, masukkan pengaturan berikut dan pilih OK:

      - Pilih tombol radio Diaktifkan.
      - Di bawah Opsi atur Opsi masuk ke Masuk otomatis hanya di zona Intranet.

5. Untuk mengaktifkan autentikasi terintegrasi, lakukan langkah-langkah berikut ini:

   a. Di alat Manajemen Kebijakan Grup, arahkan ke domain Anda, pilih Objek Kebijakan Grup, buka menu konteks (klik kanan) untuk kebijakan Pusat Identitas IAM Anda, dan pilih Edit.

   b. Di pohon kebijakan, arahkan ke Konfigurasi Pengguna > Preferensi > Pengaturan Windows.

   c. Di daftar Pengaturan Windows, buka menu konteks (klik kanan) untuk Registri dan pilih Item registri baru.

   d. Di kotak dialog Properti Registri Baru, masukkan pengaturan berikut dan pilih OK:

      Aksi

      ```
      Update
      ```

      Sarang

      ```
      HKEY_CURRENT_USER
      ```

      Jalan

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      ```

      Nama nilai

      ```
      EnableNegotiate
      ```

      Jenis nilai

      ```
      REG_DWORD
      ```

Data nilai

1

6. Tutup jendela Editor Pengelolaan Kebijakan Grup jika masih terbuka.
7. Tetapkan kebijakan baru ke domain Anda dengan mengikuti langkah-langkah berikut:
   a. Di pohon Pengelolaan Kebijakan Grup, buka menu konteks (klik kanan) untuk domain Anda, lalu pilih Menautkan GPO yang Ada.
   b. Dalam daftar Objek Kebijakan Grup, pilih kebijakan Pusat Identitas IAM Anda dan pilih OK.

Perubahan ini akan berlaku setelah pembaruan Kebijakan Grup berikutnya pada klien, atau waktu berikutnya pengguna masuk.

Sign-on tunggal untuk Firefox

Untuk mengizinkan peramban Mozilla Firefox untuk mendukung sign-on tunggal, tambahkan URL akses Anda (misalnya, https://*<alias>*.awsapps.com) ke daftar situs yang disetujui untuk sign-on tunggal. Ini bisa dilakukan secara manual, atau otomatis dengan skrip.

Topik

- Pembaruan manual untuk sign-on tunggal
- Pembaruan otomatis untuk sign-on tunggal

Pembaruan manual untuk sign-on tunggal

Untuk menambahkan URL akses Anda ke daftar situs yang disetujui di Firefox secara manual, lakukan langkah-langkah berikut pada komputer klien.

Untuk menambahkan URL akses Anda secara manual ke daftar situs yang disetujui di Firefox

1. Buka Firefox dan buka halaman `about:config`.
2. Buka preferensi `network.negotiate-auth.trusted-uris` dan tambahkan URL akses Anda ke daftar situs. Gunakan koma (,) untuk memisahkan beberapa entri.

Pembaruan otomatis untuk sign-on tunggal

Sebagai administrator domain, Anda dapat menggunakan skrip untuk menambahkan URL akses ke preferensi pengguna `network.negotiate-auth.trusted-uris` Firefox pada semua komputer di jaringan Anda. Untuk informasi selengkapnya, kunjungi https://support.mozilla.org/en-US/questions/939037.

Mengaktifkan akses ke AWS Management Console dengan kredensial AD

AWS Directory Service memungkinkan Anda untuk memberikan anggota direktori Anda akses ke AWS Management Console. Secara default, anggota direktori Anda tidak memiliki akses ke sumber daya AWS mana pun. Anda menetapkan IAM role untuk anggota direktori Anda untuk memberikan mereka akses ke berbagai layanan dan sumber daya AWS. IAM role menentukan layanan, sumber daya, dan tingkat akses yang dimiliki anggota direktori Anda.

Sebelum Anda dapat memberikan akses konsol ke anggota direktori Anda, direktori Anda harus memiliki URL akses. Untuk informasi selengkapnya tentang cara melihat detail direktori dan mendapatkan URL akses Anda, lihat Melihat informasi direktori. Untuk informasi selengkapnya tentang cara membuat URL akses, lihat Membuat URL akses.

Untuk informasi selengkapnya tentang cara membuat dan menetapkan IAM role untuk anggota direktori Anda, lihat Berikan akses ke pengguna dan grup sumber daya AWS.

Topik

- Aktifkan akses AWS Management Console
- Menonaktifkan akses AWS Management Console
- Mengatur lamanya sesi masuk

terkaitAWSArtikel Blog Keamanan

- Cara mengaksesAWS Management ConsoleMenggunakanAWSMicrosoft AD yang Dikelola dan Kredenal On-premise Anda

Aktifkan akses AWS Management Console

Secara default, akses konsol tidak diaktifkan untuk direktori apapun. Untuk mengaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk mengaktifkan akses konsol

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bawah bagian AWS Management Console, pilih Aktifkan. Akses konsol sekarang diaktifkan untuk direktori Anda.

   Sebelum pengguna dapat masuk ke konsol tersebut dengan URL akses Anda, Anda harus terlebih dahulu menambahkan pengguna Anda ke peran. Untuk informasi umum tentang menetapkan pengguna ke IAM role, lihat Menetapkan pengguna atau grup ke peran yang ada. Setelah IAM role telah ditetapkan, pengguna kemudian dapat mengakses konsol tersebut menggunakan URL akses Anda. Misalnya, jika URL akses direktori Anda adalah example-corp.awsapps.com, URL untuk mengakses konsol tersebut adalah https://example-corp.awsapps.com/console/.

Menonaktifkan akses AWS Management Console

Untuk menonaktifkan akses konsol untuk pengguna dan grup direktori Anda, lakukan langkah-langkah berikut:

Untuk menonaktifkan akses konsol

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bawah bagian AWS Management Console, pilih Menonaktifkan. Akses konsol sekarang dinonaktifkan untuk direktori Anda.
5. Jika setiap IAM role telah ditetapkan untuk pengguna atau grup dalam direktori, tombol Nonaktifkan mungkin tidak tersedia. Dalam kasus ini, Anda harus menghapus semua penetapan IAM role untuk direktori sebelum melanjutkan, termasuk tugas untuk pengguna atau grup dalam direktori Anda yang telah dihapus, yang akan ditampilkan sebagai Pengguna Dihapus atau Grup Dihapus.

   Setelah semua penetapan IAM role dihapus, ulangi langkah-langkah di atas.

Mengatur lamanya sesi masuk

Secara default, pengguna memiliki waktu 1 jam untuk menggunakan sesi mereka setelah berhasil masuk ke konsol tersebut sebelum mereka keluar. Setelah itu, pengguna harus masuk lagi untuk memulai sesi 1 jam berikutnya sebelum keluar lagi. Anda dapat menggunakan prosedur berikut untuk mengubah lama waktu hingga 12 jam per sesi.

Untuk mengatur lamanya sesi masuk

1. Pada panel navigasi konsol AWS Directory Service, pilih Direktori.
2. Pada halaman Direktori, pilih ID direktori Anda.
3. Pada halaman Detail direktori, pilih tab Pengelolaan aplikasi.
4. Di bawah bagian Aplikasi & layanan AWS, pilih Konsol Manajemen AWS.
5. Di kotak dialog Mengelola Akses ke Sumber Daya AWS, pilih Lanjutkan.
6. Di halamanMenetapkan pengguna dan grup ke IAM role, di bawah Atur lamanya sesi masuk, edit nilai bernomor, dan kemudian pilih Simpan.

Tutorial: Buat AD Sederhana Active Directory

Tutorial berikut memandu Anda melalui semua langkah yang diperlukan untuk menyiapkan Simple AD Active Directory. Ini dimaksudkan untuk membantu Anda memulai dengan Simple AD Active Directory dengan cepat dan mudah, tetapi tidak dimaksudkan untuk digunakan dalam lingkungan produksi skala besar.

Prasyarat Tutorial

Tutorial ini mengasumsikan hal berikut:

- Anda memiliki yang aktif Akun AWS.
- Akun Anda belum mencapai batas VPC Amazon untuk Wilayah tempat Anda ingin menggunakan Simple AD. Untuk informasi selengkapnya tentang VPC, lihat Apa itu Amazon VPC? dan Subnet di VPC Anda di Panduan Pengguna Amazon VPC.
- Anda tidak memiliki VPC yang ada di Wilayah dengan CIDR sebesar. `10.0.0.0/16`

Untuk informasi selengkapnya, lihat Prasyarat Simple AD.

Langkah 1: Buat dan konfigurasikan VPC Amazon Anda untuk Simple AD Active Directory

Buat dan konfigurasikan VPC Amazon untuk digunakan dengan Simple AD. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikanPrasyarat Tutorial.

Buat VPC untuk Simple AD Anda Active Directory

Buat VPC dengan dua subnet publik. AWS Directory Service membutuhkan dua subnet di VPC Anda, dan setiap subnet harus berada di Availability Zone yang berbeda.

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Di Dasbor VPC, pilih Buat VPC.
3. Di bawah pengaturan VPC, pilih VPC dan lainnya.
4. Lengkapi bidang ini sebagai berikut:
   - Tetap dibuat otomatis dipilih di bawah Generasi otomatis tag nama. Ubah proyek menjadiADS VPC.
   - Blok IPv4 CIDR seharusnya. `10.0.0.0/16`
   - Tetap pilih opsi blok CIDR IPv6 tidak dipilih.
   - Penyewaan harus tetap Default.
   - Pilih 2 untuk Jumlah Availability Zones (AZ).
   - Pilih 2 untuk Jumlah subnet publik. Jumlah subnet pribadi dapat diubah menjadi 0.
   - Pilih Sesuaikan blok CIDR subnet untuk mengonfigurasi rentang alamat IP subnet publik. Blok CIDR subnet publik harus `10.0.0.0/20` dan. `10.0.16.0/20`
5. Pilih Buat VPC. Ini akan memerlukan beberapa menit sampai VPC dibuat.

Langkah 2: Buat Direktori Aktif AD Sederhana Anda

Untuk membuat Simple AD Active Directory baru, lakukan langkah-langkah berikut. Sebelum memulai prosedur ini, pastikan Anda telah menyelesaikan prasyarat yang diidentifikasi Prasyarat Tutorial dan Langkah 1: Buat dan konfigurasikan VPC Amazon Anda untuk Simple AD. Active Directory

Untuk membuat Simple AD Active Directory

1. Di panel navigasi konsol AWS Directory Service, pilih Direktori, lalu pilih Atur direktori.

2. Di halaman Pilih jenis direktori, pilih Simple AD, lalu pilih Selanjutnya.
3. Di halaman Masukkan informasi direktori, berikan informasi berikut:

   Ukuran direktori

   Pilih salah satu opsi ukuran Small atau Large. Untuk informasi selengkapnya tentang ukuran, lihat Simple AD.

   Nama organisasi

   Sebuah nama organisasi yang unik untuk direktori Anda yang akan digunakan untuk mendaftarkan perangkat klien.

   Bidang ini hanya tersedia jika Anda membuat direktori sebagai bagian dari peluncuran WorkSpaces.

   Nama DNS direktori

   Nama berkualifikasi penuh untuk direktori, seperti `corp.example.com`.

   Direktori nama NetBIOS

   Nama singkat untuk direktori, seperti `CORP`.

   Kata sandi administrator

   Kata sandi untuk administrator direktori. Proses pembuatan direktori menciptakan akun administrator dengan nama pengguna `Administrator` dan kata sandi ini.

   Kata sandi administrator direktori peka akan huruf besar kecil dan harus terdiri dari 8 sampai 64 karakter, inklusif. Kata sandi juga harus berisi minimal satu karakter dalam tiga dari empat kategori berikut:

   - Huruf kecil (a-z)
   - Huruf besar (A-Z)
   - Angka (0-9)
   - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

   Konfirmasikan kata sandi

   Ketik ulang kata sandi administrator.

   Deskripsi direktori

   Deskripsi opsional untuk direktori.

4. Pada halaman Pilih VPC dan subnet, berikan informasi berikut ini, lalu pilih Selanjutnya.

   VPC

   VPC untuk direktori.

   Subnet

   Pilih subnet untuk pengendali domain. Kedua subnet harus berada di Zona Ketersediaan yang berbeda.
5. Pada halaman Tinjau & buat, tinjau informasi direktori dan buat perubahan yang diperlukan. Jika informasi sudah benar, pilih Buat direktori. Ini akan memerlukan beberapa menit sampai direktori dibuat. Setelah dibuat, nilai Status berubah ke Aktif.

Praktik terbaik untuk Simple AD

Berikut adalah beberapa saran dan panduan yang harus Anda pertimbangkan untuk menghindari masalah dan mendapatkan hasil maksimal dari Simple AD.

Menyiapkan: Prasyarat

Pertimbangkan panduan ini sebelum membuat direktori Anda.

Verifikasikan Anda memiliki jenis direktori yang tepat

AWS Directory Service menyediakan berbagai cara untuk digunakan dengan AWS layanan lain. Anda dapat memilih directory service dengan fitur yang Anda butuhkan dengan biaya yang sesuai dengan anggaran Anda:

- AWS Directory Service untuk Microsoft Active Directory adalah pengelola yang kaya fitur yang dihosting di cloud. AWS AWS Microsoft AD yang dikelola adalah pilihan terbaik Anda jika Anda memiliki lebih dari 5.000 pengguna dan memerlukan hubungan kepercayaan yang disiapkan antara direktori yang AWS dihosting dan direktori lokal Anda.
- AD Connector hanya menghubungkan lokal Active Directory Anda yang sudah ada. AWS AD Connector adalah pilihan terbaik Anda saat Anda ingin menggunakan direktori on-premise Anda yang sudah ada dengan layanan AWS .
- Simple AD adalah direktori berskala rendah dan berbiaya rendah dengan kompatibilitas dasarActive Directory. Ini mendukung 5.000 atau lebih sedikit pengguna, aplikasi yang kompatibel dengan Samba 4, dan kompatibilitas LDAP untuk aplikasi sadar LDAP.

Untuk perbandingan AWS Directory Service opsi yang lebih rinci, lihatMana yang harus dipilih.

Pastikan VPC dan instans Anda dikonfigurasi dengan benar

Untuk terhubung ke, mengelola, dan menggunakan direktori Anda, Anda harus mengkonfigurasi VPC yang terkait direktori dengan benar. Lihat AWS Prasyarat Microsoft AD yang dikelola, Prasyarat AD Connector, atau Prasyarat Simple AD untuk informasi tentang persyaratan keamanan dan jaringan VPC.

Jika Anda menambahkan instans ke domain Anda, pastikan bahwa Anda memiliki konektivitas dan akses jarak jauh ke instans Anda seperti yang dijelaskan di Bergabunglah dengan instans Amazon EC2 ke Direktori Aktif AWS Microsoft AD Terkelola.

Ketahui batasan Anda

Pelajari tentang berbagai batasan untuk jenis direktori spesifik Anda. Penyimpanan yang tersedia dan ukuran agregat objek Anda adalah satu-satunya keterbatasan terkait jumlah objek yang dapat Anda simpan dalam direktori Anda. Lihat Kuota Microsoft AD yang Dikelola AWS, Kuota AD Connector, atau Kuota Simple AD untuk detail tentang direktori pilihan Anda.

Pahami konfigurasi grup AWS keamanan direktori Anda dan gunakan

AWS membuat grup keamanan dan melampirkannya ke antarmuka jaringan elastis pengontrol domain direktori Anda. AWS mengkonfigurasi grup keamanan untuk memblokir lalu lintas yang tidak perlu ke direktori dan memungkinkan lalu lintas yang diperlukan.

Memodifikasi grup keamanan direktori

Jika Anda ingin mengubah keamanan grup keamanan direktori Anda, Anda dapat melakukannya. Hanya buat perubahan tersebut jika Anda sepenuhnya memahami cara kerja filter grup keamanan. Untuk informasi selengkapnya, lihat Grup Keamanan Amazon EC2 untuk instans Linux di Panduan Pengguna Amazon EC2. Perubahan yang tidak tepat dapat mengakibatkan hilangnya komunikasi ke komputer dan instance yang dituju. AWS merekomendasikan agar Anda tidak mencoba membuka port tambahan ke direktori Anda karena ini mengurangi keamanan direktori Anda. Harap tinjau dengan seksama Model Tanggung Jawab Bersama AWS.

> **Warning**
>
> Secara teknis Anda dapat mengasosiasikan grup keamanan direktori dengan instans EC2 lain yang Anda buat. Namun, AWS merekomendasikan untuk tidak melakukan praktik ini. AWS mungkin memiliki alasan untuk memodifikasi grup keamanan tanpa pemberitahuan

untuk mengatasi kebutuhan fungsional atau keamanan direktori terkelola. Perubahan tersebut mempengaruhi setiap instans yang Anda asosiasikan dengan grup keamanan direktori dan dapat mengganggu operasi instans terkait. Selain itu, mengaitkan grup keamanan direktori dengan instans EC2 Anda dapat menciptakan risiko keamanan potensial untuk instans EC2 Anda.

Gunakan Microsoft AD yang AWS Dikelola jika diperlukan kepercayaan

Simple AD tidak mendukung hubungan kepercayaan. Jika Anda perlu membangun kepercayaan antara AWS Directory Service direktori Anda dan direktori lain, Anda harus menggunakan AWS Directory Service untuk Microsoft Active Directory.

Pengaturan: Membuat direktori Anda

Berikut adalah beberapa saran untuk dipertimbangkan saat Anda membuat direktori Anda.

Ingat ID dan kata sandi administrator Anda

Saat mengatur direktori Anda, Anda memberikan kata sandi untuk akun administrator. ID akun tersebut adalah Administrator untuk Simple AD. Ingat kata sandi yang Anda buat untuk akun ini; jika tidak, Anda tidak akan dapat menambahkan objek ke direktori Anda.

Memahami batasan nama pengguna untuk AWS aplikasi

AWS Directory Service memberikan dukungan untuk sebagian besar format karakter yang dapat digunakan dalam pembangunan nama pengguna. Namun, ada batasan karakter yang diberlakukan pada nama pengguna yang akan digunakan untuk masuk ke AWS aplikasi, seperti, Amazon, WorkSpaces WorkDocs Amazon WorkMail, atau Amazon. QuickSight Pembatasan ini mengharuskan karakter berikut tidak digunakan:

- Spasi
- Karakter multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Simbol @ diperbolehkan selama itu mendahului akhiran UPN.

Memprogram aplikasi Anda

Sebelum memprogram aplikasi Anda, pertimbangkan hal berikut:

Menggunakan layanan locator Windows DC

Saat mengembangkan aplikasi, gunakan layanan pencari lokasi Windows DC atau gunakan layanan Dynamic DNS (DDNS) dari AWS Microsoft AD yang Dikelola untuk menemukan pengontrol domain (DC). Jangan hard code aplikasi dengan alamat DC. Layanan locator DC membantu memastikan beban direktori didistribusikan dan memungkinkan Anda untuk mengambil keuntungan dari penskalaan horizontal dengan menambahkan pengendali domain untuk deployment Anda. Jika Anda mengikat aplikasi ke DC tetap dan DC mengalami patch atau pemulihan, aplikasi Anda akan kehilangan akses ke DC bukannya menggunakan salah satu DC yang tersisa. Selain itu, hard coding DC dapat mengakibatkan hot spotting pada DC tunggal. Pada kasus yang parah, hot spotting dapat menyebabkan DC Anda menjadi tidak responsif. Kasus seperti itu juga dapat menyebabkan otomatisasi AWS direktori menandai direktori sebagai terganggu dan dapat memicu proses pemulihan yang menggantikan DC yang tidak responsif.

Muat tes sebelum diluncurkan ke produksi

Pastikan untuk melakukan pengujian laboratorium dengan aplikasi dan permintaan yang mewakili beban kerja produksi Anda untuk mengonfirmasi bahwa direktori menskalakan ke beban aplikasi Anda. Jika Anda memerlukan kapasitas tambahan, Anda harus menggunakan AWS Directory Service Microsoft Active Directory, yang memungkinkan Anda menambahkan pengontrol domain untuk kinerja tinggi. Untuk informasi selengkapnya, lihat Men-deploy pengendali domain tambahan.

Gunakan kueri LDAP yang efisien

Kueri LDAP luas ke pengendali domain pada ribuan objek dapat mengkonsumsi siklus CPU yang signifikan dalam DC tunggal, mengakibatkan hot spotting. Hal ini dapat mempengaruhi aplikasi yang berbagi DC yang sama selama kueri.

Kuota Simple AD

Umumnya, Anda tidak harus menambahkan lebih dari 500 pengguna ke direktori Simple AD Small dan tidak lebih dari 5.000 pengguna ke direktori AD sederhana Large. Untuk opsi skala yang lebih fleksibel dan fitur Direktori Aktif tambahan, pertimbangkan untuk menggunakan Directory Service AWS untuk Microsoft Active Directory (Edisi Standar atau Edisi Enterprise).

Berikut ini adalah kuota default untuk Simple AD. Kecuali dinyatakan lain, masing-masing kuota adalah per Region.

Kuota Simple AD

Resource	Kuota default
Direktori Simple AD	10
Snapshot manual *	5 per Simple AD

* Kuota snapshot manual tidak dapat diubah.

> **Note**
>
> Anda tidak dapat melampirkan alamat IP publik ke elastic network interface (ENI) AWS Anda.

Kebijakan kompatibilitas aplikasi untuk Simple AD

Simple AD merupakan implementasi dari Samba yang menyediakan banyak fitur dasar Direktori Aktif. Karena besarnya aplikasi siap pakai khusus dan komersial yang menggunakan Direktori Aktif, AWS tidak dan tidak dapat melakukan verifikasi formal atau luas dari kompatibilitas aplikasi pihak ketiga dengan Simple AD. Meskipun AWS bekerja dengan pelanggan dalam upaya mengatasi potensi tantangan instalasi aplikasi yang mungkin mereka hadapi, kami tidak dapat menjamin bahwa aplikasi apa pun adalah atau akan terus kompatibel dengan Simple AD.

Aplikasi pihak ketiga berikut ini kompatibel dengan Simple AD:

- Microsoft Internet Information Services (IIS) pada platform berikut:
  - Windows Server 2003 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Microsoft SQL Server:
  - SQL Server 2005 R2 (edisi Ekspres, Web, dan Standar)

  - SQL Server 2008 R2 (edisi Ekspres, Web, dan Standar)
  - SQL Server 2012 (edisi Ekspres, Web, dan Standar)
  - SQL Server 2014 (edisi Ekspres, Web, dan Standar)
- Microsoft SharePoint:
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

Pelanggan dapat memilih untuk menggunakan Directory Service AWS untuk Microsoft Active Directory (AWS Microsoft AD yang dikelola) untuk tingkat kompatibilitas yang lebih tinggi berdasarkan Direktori Aktif sebenarnya.

Pemecahan masalah Simple AD

Berikut ini dapat membantu Anda memecahkan beberapa masalah umum yang mungkin Anda alami saat membuat atau menggunakan direktori Anda.

Topik

Pemulihan kata sandi

Jika pengguna lupa kata sandi atau mengalami masalah saat masuk ke direktori Simple AD atau Microsoft AD yang AWS Dikelola, Anda dapat mengatur ulang kata sandi mereka menggunakan direktori AWS Management Console, Windows PowerShell atau direktori. AWS CLI

Untuk informasi selengkapnya, lihat Mengatur ulang kata sandi pengguna.

Saya menerima kesalahan “KDC tidak dapat memenuhi opsi yang diminta” saat menambahkan pengguna ke Simple AD

Hal ini dapat terjadi ketika klien Samba CLI tidak mengirim perintah 'bersih' dengan benar untuk semua pengendali domain. Jika Anda melihat pesan kesalahan ini saat menggunakan perintah 'iklan bersih' untuk menambahkan pengguna ke direktori Simple AD, gunakan argumen -S dan tentukan alamat IP salah satu pengontrol domain Anda. Jika Anda masih melihat kesalahan, coba pengendali domain lainnya. Anda juga dapat menggunakan Alat Administrasi Direktori Aktif untuk menambahkan pengguna ke direktori Anda. Untuk informasi selengkapnya, lihat Instal Alat Administrasi Direktori Aktif untuk Simple AD.

Saya tidak dapat memperbarui nama DNS atau alamat IP instans bergabung ke domain saya (pembaruan dinamis DNS).

Pembaruan dinamis DNS tidak didukung di domain Simple AD. Sebagai gantinya Anda dapat membuat perubahan secara langsung dengan menghubungkan ke direktori Anda menggunakan Pengelola DNS pada instans yang digabungkan ke domain Anda.

Saya tidak dapat masuk ke SQL Server menggunakan akun SQL Server

Anda mungkin menerima kesalahan jika mencoba menggunakan SQL Server Management Studio (SSMS) dengan akun SQL Server untuk masuk ke SQL Server yang berjalan pada instans Windows 2012 R2 EC2. Masalah terjadi ketika SSMS berjalan sebagai pengguna domain dan dapat mengakibatkan kesalahan “Login gagal untuk pengguna,” bahkan ketika kredensi yang valid disediakan. Ini adalah masalah yang diketahui dan AWS secara aktif bekerja untuk menyelesaikannya.

Untuk mengatasi masalah ini, Anda dapat masuk ke SQL Server dengan Autentikasi Windows bukan Autentikasi SQL. Atau luncurkan SSMS sebagai pengguna lokal, bukan pengguna domain Simple AD.

Direktori saya terjebak dalam status “diminta”

Jika Anda memiliki direktori yang telah berada dalam status “Diminta” selama lebih dari lima menit, coba hapus direktori dan buat ulang. Jika masalah ini berlanjut, kontak Pusat AWS Support.

Saya menerima kesalahan “AZ dibatasi” saat saya membuat direktori

Beberapa AWS akun yang dibuat sebelum 2012 mungkin memiliki akses ke Availability Zones di AS Timur (Virginia N.), AS Barat (California N.), atau Wilayah Asia Pasifik (Tokyo) yang tidak mendukung AWS Directory Service direktori. Jika Anda menerima kesalahan seperti ini saat membuat direktori, pilih subnet di Availability Zone yang berbeda dan coba untuk membuat direktori lagi.

Beberapa pengguna saya tidak dapat mengautentikasi dengan direktori saya

Akun pengguna Anda harus mengaktifkan pra-autentikasi Kerberos. Ini adalah pengaturan default untuk akun pengguna baru, dan seharusnya tidak diubah. Untuk informasi selengkapnya tentang pengaturan ini, buka Preauthentication di Microsoft. TechNet

Sumber daya tambahan

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengannya. AWS

- AWS Pusat Pengetahuan —Temukan FAQ dan tautan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- AWS Support Center —Dapatkan dukungan teknis.
- AWS Pusat Support Premium —Dapatkan dukungan teknis premium.

Topik

- Alasan status direktori Simple AD

Alasan status direktori Simple AD

Ketika direktori terganggu atau tidak bisa dioperasi, pesan status direktori berisi informasi tambahan. Pesan status ditampilkan dalam konsol AWS Directory Service, atau dikembalikan di anggota

`DirectoryDescription.StageReason` oleh API `DescribeDirectories`. Untuk informasi selengkapnya tentang status direktori, lihat Memahami status direktori Anda.

Berikut ini adalah pesan status untuk direktori Simple AD:

Topik

- Antarmuka jaringan elastis layanan direktori tidak terpasang
- Masalah terdeteksi oleh instans
- Pengguna yang disimpan AWS Directory Service kritis hilang dari direktori
- Pengguna yang disimpan AWS Directory Service kritis harus menjadi milik grup Admin Domain
- Pengguna yang disimpan AWS Directory Service kritis dinonaktifkan
- Pengendali domain utama tidak memiliki semua peran FSMO
- Kegagalan replikasi pengendali domain

Antarmuka jaringan elastis layanan direktori tidak terpasang

Deskripsi

antarmuka jaringan elastis (ENI) kritis yang dibuat atas nama Anda selama pembuatan direktori untuk membangun konektivitas jaringan dengan VPC Anda tidak terlampir pada instans direktori. Aplikasi AWS yang didukung oleh direktori ini tidak akan berfungsi. Direktori Anda tidak dapat terhubung ke jaringan on-premise Anda.

Pemecahan Masalah

Jika ENI terlepas tapi masih ada, hubungi AWS Support. Jika ENI dihapus, tidak ada cara untuk menyelesaikan masalah tersebut dan direktori Anda secara permanen tidak dapat digunakan. Anda harus menghapus direktori tersebut dan membuat direktori baru.

Masalah terdeteksi oleh instans

Deskripsi

Kesalahan internal terdeteksi oleh instans. Hal ini biasanya menandakan bahwa layanan pemantauan mencoba untuk memulihkan secara aktif instans yang terganggu.

Pemecahan Masalah

Dalam kebanyakan kasus, ini adalah masalah sementara, dan direktori akhirnya kembali ke keadaan Aktif. Jika masalah berlanjut, hubungi AWS Support untuk mendapatkan bantuan lebih lanjut.

Pengguna yang disimpan AWS Directory Service kritis hilang dari direktori

Deskripsi

Ketika Simple AD dibuat, AWS Directory Service membuat akun layanan di direktori dengan nama `AWSAdmin`*`D-xxxxxxxxx`*. Kesalahan ini diterima saat akun layanan ini tidak dapat ditemukan. Tanpa akun ini, AWS Directory Service tidak dapat melakukan fungsi administratif pada direktori, rendering direktori tidak dapat digunakan.

Pemecahan Masalah

Untuk memperbaiki masalah ini, pulihkan direktori ke snapshot sebelumnya yang dibuat sebelum akun layanan dihapus. Snapshot otomatis diambil dari direktori Simple AD Anda satu kali sehari. Jika sudah lebih dari lima hari setelah akun ini dihapus, Anda mungkin tidak dapat memulihkan direktori ke keadaan di mana akun ini berada. Jika Anda tidak dapat memulihkan direktori dari snapshot di mana akun ini berada, direktori Anda mungkin menjadi tidak dapat digunakan secara permanen. Jika ini adalah kasusnya, Anda harus menghapus direktori Anda dan membuat direktori baru.

Pengguna yang disimpan AWS Directory Service kritis harus menjadi milik grup Admin Domain

Deskripsi

Ketika Simple AD dibuat, AWS Directory Service membuat akun layanan di direktori dengan nama `AWSAdmin`*`D-xxxxxxxxx`*. Kesalahan ini diterima saat akun layanan ini bukan anggota dari grup `Domain Admins`. Keanggotaan dalam grup ini diperlukan untuk memberikan AWS Directory Service hak istimewa yang dibutuhkan untuk melakukan operasi pemeliharaan dan pemulihan, seperti mentransfer peran FSMO, menggabungkan domain pengendali direktori baru, dan memulihkan dari snapshot.

Pemecahan Masalah

Menggunakan alat Pengguna dan Komputer Direktori Aktif untuk menambahkan akun layanan ke grup `Domain Admins`.

Pengguna yang disimpan AWS Directory Service kritis dinonaktifkan

Deskripsi

Ketika Simple AD dibuat, AWS Directory Service membuat akun layanan di direktori dengan nama `AWSAdmin`*`D-xxxxxxxxx`*. Kesalahan ini diterima saat akun layanan ini dinonaktifkan. Akun ini harus diaktifkan sehingga AWS Directory Service dapat melakukan operasi pemeliharaan dan pemulihan pada direktori.

Pemecahan Masalah

Menggunakan alat Pengguna dan Komputer Direktori Aktif untuk mengaktifkan kembali akun layanan.

Pengendali domain utama tidak memiliki semua peran FSMO

Deskripsi

Semua peran FSMO tidak dimiliki oleh pengendali direktori Simple AD. AWS Directory Service tidak dapat menjamin perilaku tertentu dan fungsi jika peran FSMO tidak milik pengendali direktori Simple AD yang benar.

Pemecahan Masalah

Menggunakan alat Direktori Aktif untuk memindahkan peran FSMO kembali ke pengendali direktori kerja asli. Untuk informasi selengkapnya tentang memindahkan peran FSMO, kunjungi https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. Jika ini tidak memperbaiki masalah, silakan hubungi AWS Support untuk mendapatkan bantuan lebih lanjut.

Kegagalan replikasi pengendali domain

Deskripsi

Pengendali direktori Simple AD gagal untuk mereplikasi dengan satu sama lain. Hal ini dapat disebabkan oleh satu atau beberapa masalah berikut:

- Grup keamanan untuk pengendali direktori tidak memiliki port-port yang benar terbuka.
- ACL jaringan terlalu membatasi.
- Tabel rute VPC tidak merutekan lalu lintas jaringan antara pengendali direktori dengan benar.
- Instans lain telah dipromosikan ke pengendali domain di direktori.

Pemecahan Masalah

Untuk informasi selengkapnya tentang persyaratan jaringan VPC Anda, lihat salah satuAWSDikelola Microsoft ADAWS Prasyarat Microsoft AD yang dikelola, AD ConnectorPrasyarat AD Connector, atau Simple ADPrasyarat Simple AD. Jika ada pengendali domain yang tidak dikenal di direktori Anda, Anda harus menurunkannya. Jika pengaturan jaringan VPC Anda benar, tetapi kesalahan tetap ada, silakan hubungi AWS Support untuk mendapatkan bantuan lebih lanjut.

Keamanan di AWS Directory 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 menjelaskan 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. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari AWS program kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku AWS Directory Service, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

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

Topik keamanan

Topik keamanan berikut dapat ditemukan di bagian ini:

- Identitas dan manajemen akses untuk AWS Directory Service
- Penebangan dan pemantauan di AWS Directory Service
- Validasi kepatuhan untuk AWS Directory Service
- Ketahanan di AWS Directory Service
- Keamanan infrastruktur di AWS Directory Service

Topik keamanan tambahan

Topik keamanan tambahan berikut dapat ditemukan dalam panduan ini:

Akun, trust, dan akses AWS sumber daya

- Izin untuk akun Administrator
- Akun Layanan yang Dikelola Grup
- Menciptakan hubungan kepercayaan
- Delegasi terbatas Kerberos
- Berikan akses ke pengguna dan grup sumber daya AWS
- Otorisasi untuk AWS aplikasi dan layanan menggunakan AWS Directory Service

Amankan direktori Anda

- Mengamankan direktori Microsoft AD yang Dikelola AWS Anda
- Mengamankan direktori AD Connector Anda

Pencatatan dan pemantauan

- Memantau Microsoft AD yang Dikelola AWS Anda
- Memantau direktori AD Connector Anda

Ketahanan

- Patching dan pemeliharaan Microsoft AD yang Dikelola AWS

Identitas dan manajemen akses untuk AWS Directory Service

Akses ke AWS Directory Service memerlukan kredensyal yang AWS dapat digunakan untuk mengautentikasi permintaan Anda. Kredensyal tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti direktori. AWS Directory Service Bagian berikut memberikan rincian tentang bagaimana Anda dapat menggunakan AWS Identity and Access Management (IAM) dan AWS Directory Service untuk membantu mengamankan sumber daya Anda dengan mengontrol siapa yang dapat mengaksesnya:

- Autentikasi

- Kontrol akses

Autentikasi

Pelajari cara mengakses AWS menggunakan identitas IAM.

Kontrol akses

Anda dapat memiliki kredensi yang valid untuk mengautentikasi permintaan Anda, tetapi kecuali Anda memiliki izin, Anda tidak dapat membuat atau mengakses sumber daya. AWS Directory Service Misalnya, Anda harus memiliki izin untuk membuat AWS Directory Service direktori atau membuat snapshot direktori.

Bagian berikut menjelaskan cara mengelola izin untuk AWS Directory Service. Anda disarankan untuk membaca gambaran umum terlebih dahulu.

- Ikhtisar mengelola izin akses ke sumber daya Anda AWS Directory Service
- Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Directory Service
- AWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi

Ikhtisar mengelola izin akses ke sumber daya Anda AWS Directory Service

Setiap AWS sumber daya dimiliki oleh AWS akun, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin. Administrator akun dapat melampirkan kebijakan izin ke identitas IAM (yaitu, pengguna, grup, dan peran), dan beberapa layanan (seperti AWS Lambda) juga mendukung melampirkan kebijakan izin ke sumber daya.

> **Note**
>
> Administrator akun (atau pengguna administrator) adalah pengguna dengan hak akses administrator. Untuk informasi selengkapnya, lihat Praktik terbaik IAM dalam Panduan Pengguna IAM.

Topik

- AWS Directory Service sumber daya dan operasi
- Memahami kepemilikan sumber daya
- Mengelola akses ke sumber daya
- Menentukan elemen kebijakan: Tindakan, efek, sumber daya, dan prinsipal
- Menentukan kondisi dalam kebijakan

AWS Directory Service sumber daya dan operasi

Di AWS Directory Service, sumber daya utama adalah direktori. AWS Directory Service mendukung sumber daya snapshot direktori juga. Namun, Anda dapat membuat snapshot hanya dalam konteks direktori yang ada. Oleh karena itu, snapshot disebut sebagai Subsumber daya.

Sumber daya ini memiliki Amazon Resource Name (ARN) unik yang terkait dengan mereka, seperti yang ditunjukkan di tabel berikut.

Jenis Sumber Daya	Format ARN
Direktori	`arn:aws:ds: region:account-id :directory/ external-directory-id`
Snapshot	`arn:aws:ds: region:account-id :snapshot/ external-snapshot-id`

AWS Directory Service menyediakan satu set operasi untuk bekerja dengan sumber daya yang sesuai. Untuk daftar operasi yang tersedia, lihat Tindakan Directory Service.

Memahami kepemilikan sumber daya

Pemilik sumber daya adalah AWS akun yang membuat sumber daya. Artinya, pemilik sumber daya adalah AWS akun entitas utama (akun root, pengguna IAM, atau peran IAM) yang mengautentikasi permintaan yang membuat sumber daya. Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensi akun root AWS akun Anda untuk membuat AWS Directory Service sumber daya, seperti direktori, AWS akun Anda adalah pemilik sumber daya tersebut.
- Jika Anda membuat pengguna IAM di AWS akun Anda dan memberikan izin untuk membuat AWS Directory Service sumber daya kepada pengguna tersebut, pengguna juga dapat membuat AWS

Directory Service sumber daya. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya.

- Jika Anda membuat peran IAM di AWS akun Anda dengan izin untuk membuat AWS Directory Service sumber daya, siapa pun yang dapat mengambil peran tersebut dapat membuat AWS Directory Service sumber daya. AWS Akun Anda, tempat peran itu berada, memiliki AWS Directory Service sumber daya.

Mengelola akses ke sumber daya

Kebijakan izin menjelaskan siapa yang memiliki akses ke suatu objek. Bagian berikut menjelaskan opsi yang tersedia untuk membuat kebijakan izin.

> **Note**
>
> Bagian ini membahas penggunaan IAM dalam konteks. AWS Directory Service Bagian ini tidak memberikan informasi yang mendetail tentang layanan IAM. Untuk dokumentasi lengkap IAM, lihat Apa yang Dimaksud dengan IAM? dalam Panduan Pengguna IAM. Untuk informasi tentang sintaksis dan penjelasan kebijakan IAM, lihat Referensi Kebijakan IAM JSON dalam Panduan Pengguna IAM.

Kebijakan yang melekat pada identitas IAM disebut sebagai kebijakan berbasis identitas (kebijakan IAM) dan kebijakan yang melekat pada sumber daya disebut sebagai kebijakan berbasis sumber daya. AWS Directory Service hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Topik

- Kebijakan berbasis identitas (kebijakan IAM)
- Kebijakan berbasis sumber daya

Kebijakan berbasis identitas (kebijakan IAM)

Anda dapat melampirkan kebijakan ke identitas IAM Anda. Misalnya, Anda dapat melakukan hal berikut:

- Lampirkan kebijakan izin ke pengguna atau grup di akun Anda — Administrator akun dapat menggunakan kebijakan izin yang dikaitkan dengan pengguna tertentu untuk memberikan izin bagi pengguna tersebut untuk membuat AWS Directory Service sumber daya, seperti direktori baru.

- Melampirkan kebijakan izin pada peran (memberikan izin lintas akun) – Anda dapat melampirkan kebijakan izin berbasis identitas ke peran IAM untuk memberikan izin lintas akun.

  Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mendelegasikan izin, lihat Manajemen Akses dalam Panduan Pengguna IAM.

Kebijakan izin berikut memberikan izin kepada pengguna untuk menjalankan semua tindakan yang dimulai dengan `Describe`. Tindakan ini menampilkan informasi tentang AWS Directory Service sumber daya, seperti direktori atau snapshot. Perhatikan bahwa karakter wildcard (*) dalam `Resource` elemen menunjukkan bahwa tindakan diizinkan untuk semua AWS Directory Service sumber daya yang dimiliki oleh akun.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Untuk informasi selengkapnya tentang menggunakan kebijakan berbasis identitas dengan AWS Directory Service, lihat. Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Directory Service Untuk informasi lebih lanjut tentang pengguna, kelompok, peran, dan izin, lihat Identitas (Pengguna, Grup, dan Peran) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Layanan lain, seperti Amazon S3, juga mendukung kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. AWS Directory Service tidak mendukung kebijakan berbasis sumber daya.

Menentukan elemen kebijakan: Tindakan, efek, sumber daya, dan prinsipal

Untuk setiap AWS Directory Service sumber daya, layanan mendefinisikan satu set operasi API. Untuk informasi selengkapnya, lihat AWS Directory Service sumber daya dan operasi. Untuk daftar operasi API yang tersedia, lihat Tindakan Directory Service.

Untuk memberikan izin untuk operasi API ini, AWS Directory Service tentukan serangkaian tindakan yang dapat Anda tentukan dalam kebijakan. Perhatikan bahwa melakukan operasi API bisa memerlukan izin untuk lebih dari satu tindakan.

Berikut ini adalah elemen-elemen kebijakan dasar:

- Sumber Daya - Dalam kebijakan, Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang menerapkan kebijakan tersebut. Untuk AWS Directory Service sumber daya, Anda selalu menggunakan karakter wildcard (*) dalam kebijakan IAM. Untuk informasi selengkapnya, lihat AWS Directory Service sumber daya dan operasi.
- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak. Misalnya, izin `ds:DescribeDirectories` memungkinkan pengguna untuk melakukan AWS Directory Service `DescribeDirectories` operasi.
- Pengaruh – Anda menentukan pengaruh saat pengguna meminta tindakan tertentu. Hal ini bisa berupa mengizinkan atau menolak. Jika Anda tidak secara eksplisit memberikan akses untuk (mengizinkan) sumber daya, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun kebijakan yang berbeda memberikan akses.
- Principal – Dalam kebijakan berbasis identitas (Kebijakan IAM), pengguna yang kebijakannya terlampir adalah principal yang implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang ingin Anda terima izin (hanya berlaku untuk kebijakan berbasis sumber daya). AWS Directory Service tidak mendukung kebijakan berbasis sumber daya.

Untuk mempelajari sintaksis dan penjelasan kebijakan IAM selengkapnya, lihat Referensi Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk tabel yang menunjukkan semua tindakan AWS Directory Service API dan sumber daya yang diterapkan, lihatAWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi.

Menentukan kondisi dalam kebijakan

Ketika Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan akses untuk menentukan syarat kapan kebijakan akan berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan, lihat Kondisi dalam Panduan Pengguna IAM.

Untuk menyatakan kondisi, Anda menggunakan kunci kondisi standar. Tidak ada kunci syarat khusus untuk AWS Directory Service. Namun, ada tombol AWS kondisi yang dapat Anda gunakan sesuai kebutuhan. Untuk daftar lengkap AWS kunci, lihat Kunci kondisi global yang tersedia di Panduan Pengguna IAM.

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Directory Service

Topik ini memberikan contoh kebijakan berbasis identitas di mana administrator akun dapat melampirkan kebijakan izin ke identitas IAM (yaitu, pengguna, grup, dan peran).

> **Important**
>
> Kami menyarankan Anda terlebih dahulu meninjau topik pengantar yang menjelaskan konsep dasar dan opsi yang tersedia bagi Anda untuk mengelola akses ke AWS Directory Service sumber daya Anda. Untuk informasi selengkapnya, lihat Ikhtisar mengelola izin akses ke sumber daya Anda AWS Directory Service.

Bagian dalam topik ini mencakup hal berikut:

- Izin diperlukan untuk menggunakan konsol AWS Directory Service
- AWS kebijakan terkelola (standar) untuk AWS Directory Service
- Contoh kebijakan yang dikelola pelanggan
- Menggunakan tanda dengan kebijakan IAM

Berikut adalah contoh kebijakan izin.

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDsEc2IamGetRole",
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ec2:RevokeSecurityGroupIngress",
```

```
                "ec2:CreateNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "iam:GetRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
        },
        {
            "Sid": "AllowPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

Kebijakannya meliputi hal berikut:

- Pernyataan pertama memberikan izin untuk membuat AWS Directory Service direktori. AWS Directory Service tidak mendukung izin untuk tindakan khusus ini di tingkat sumber daya. Oleh karena itu, kebijakan menentukan karakter wildcard (*) sebagai nilai `Resource`.

- Pernyataan kedua memberikan izin untuk tindakan IAM tertentu. Akses ke tindakan IAM diperlukan agar AWS Directory Service dapat membaca dan membuat peran IAM atas nama Anda. Karakter wildcard (*) di akhir nilai `Resource` berarti bahwa pernyataan itu memungkinkan izin untuk tindakan IAM di setiap IAM role. Untuk membatasi izin ini ke peran tertentu, ganti karakter wildcard (*) di ARN sumber daya dengan nama peran tertentu. Untuk informasi selengkapnya, lihat Tindakan IAM.
- Pernyataan ketiga memberikan izin ke kumpulan sumber daya Amazon EC2 tertentu yang diperlukan untuk AWS Directory Service memungkinkan membuat, mengonfigurasi, dan menghancurkan direktorinya. Karakter wildcard (*) di akhir nilai `Resource` berarti bahwa pernyataan itu memungkinkan izin untuk tindakan EC2 di setiap sumber daya atau sub-sumber daya EC2. Untuk membatasi izin ini ke peran tertentu, ganti karakter wildcard (*) di ARN sumber daya dengan sumber daya atau subsumber daya tertentu. Untuk informasi selengkapnya, lihat Tindakan Amazon EC2.

Kebijakan tersebut tidak menyebutkan elemen `Principal` karena dalam kebijakan berbasis identitas, Anda tidak menentukan prinsipal yang mendapatkan izin. Saat Anda menyematkan kebijakan kepada pengguna, pengguna ini menjadi pengguna utama implisit. Saat Anda menyematkan kebijakan izin pada peran IAM, pengguna utama yang diidentifikasi dalam kebijakan kepercayaan peran tersebut akan mendapatkan izin.

Untuk tabel yang menunjukkan semua tindakan AWS Directory Service API dan sumber daya yang diterapkan, lihatAWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi.

Izin diperlukan untuk menggunakan konsol AWS Directory Service

Agar pengguna dapat bekerja dengan AWS Directory Service konsol, pengguna tersebut harus memiliki izin yang tercantum dalam kebijakan sebelumnya atau izin yang diberikan oleh peran Directory Service Full Access Role atau Directory Service Read Only, yang dijelaskan dalam. AWS kebijakan terkelola (standar) untuk AWS Directory Service

Jika Anda membuat kebijakan IAM yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya bagi pengguna dengan kebijakan IAM tersebut.

AWS kebijakan terkelola (standar) untuk AWS Directory Service

AWS mengatasi banyak kasus penggunaan umum dengan menyediakan kebijakan IAM mandiri yang dibuat dan dikelola oleh. AWS Kebijakan terkelola memberikan izin yang diperlukan untuk kasus

penggunaan umum sehingga Anda tidak perlu menyelidiki izin apa yang diperlukan. Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

Kebijakan AWS terkelola berikut, yang dapat Anda lampirkan ke pengguna di akun Anda, khusus untuk AWS Directory Service:

- AWSDirectoryServiceReadOnlyAccess— Memberikan pengguna atau grup akses hanya-baca ke semua AWS Directory Service sumber daya, subnet EC2, antarmuka jaringan EC2, dan topik dan langganan Amazon Simple Notification Service (Amazon SNS) untuk akun root. AWS Untuk informasi selengkapnya, lihat Menggunakan kebijakan yang dikelola AWS dengan AWS Directory Service.
- AWSDirectoryServiceFullAccess— Memberikan pengguna atau grup berikut ini:
  - Akses penuh ke AWS Directory Service
  - Akses ke layanan Amazon EC2 utama yang diperlukan untuk digunakan AWS Directory Service
  - Kemampuan untuk membuat daftar topik Amazon SNS
  - Kemampuan untuk membuat, mengelola, dan menghapus topik Amazon SNS dengan nama yang diawali dengan “” DirectoryMonitoring

  Untuk informasi selengkapnya, lihat Menggunakan kebijakan yang dikelola AWS dengan AWS Directory Service.

Selain itu, ada kebijakan AWS terkelola lainnya yang cocok untuk digunakan dengan peran IAM lainnya. Kebijakan ini ditetapkan ke peran yang terkait dengan pengguna di AWS Directory Service direktori Anda. Kebijakan ini diperlukan agar pengguna tersebut memiliki akses ke AWS sumber daya lain, seperti Amazon EC2. Untuk informasi selengkapnya, lihat Berikan akses ke pengguna dan grup sumber daya AWS.

Anda juga dapat membuat kebijakan IAM khusus yang mengizinkan pengguna untuk mengakses tindakan dan sumber daya API yang diperlukan. Anda dapat melampirkan kebijakan khusus ini ke pengguna IAM atau grup yang memerlukan izin tersebut.

Contoh kebijakan yang dikelola pelanggan

Di bagian ini, Anda dapat menemukan contoh kebijakan pengguna yang memberikan izin untuk berbagai AWS Directory Service tindakan.

> **Note**
>
> Semua contoh menggunakan Region US West (Oregon) (`us-west-2`) dan berisi ID akun fiktif.

Contoh-contoh

- Contoh 1: Izinkan pengguna melakukan tindakan Deskripsikan apa pun pada AWS Directory Service sumber daya apa pun
- Contoh 2: Mengizinkan pengguna untuk membuat direktori

Contoh 1: Izinkan pengguna melakukan tindakan Deskripsikan apa pun pada AWS Directory Service sumber daya apa pun

Kebijakan izin berikut memberikan izin kepada pengguna untuk menjalankan semua tindakan yang dimulai dengan `Describe`. Tindakan ini menampilkan informasi tentang AWS Directory Service sumber daya, seperti direktori atau snapshot. Perhatikan bahwa karakter wildcard (*) dalam `Resource` elemen menunjukkan bahwa tindakan diizinkan untuk semua AWS Directory Service sumber daya yang dimiliki oleh akun.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Contoh 2: Mengizinkan pengguna untuk membuat direktori

Kebijakan izin berikut memberikan izin untuk memungkinkan pengguna untuk membuat direktori dan semua sumber daya terkait lainnya, seperti snapshot dan trust. Untuk melakukannya, izin untuk layanan Amazon EC2 tertentu juga diperlukan.

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

```
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
         "Resource":"*"
         ]
      }
   ]
}
```

Menggunakan tanda dengan kebijakan IAM

Anda dapat menerapkan izin tingkat sumber daya berbasis tag dalam kebijakan IAM yang Anda gunakan untuk sebagian besar tindakan API. AWS Directory Service Hal ini memberi Anda kontrol yang lebih baik atas sumber daya yang dapat dibuat, dimodifikasi, atau digunakan oleh pengguna. Anda menggunakan elemen `Condition` (juga disebut blok `Condition`) dengan kunci konteks syarat berikut dan nilai-nilai dalam kebijakan IAM untuk mengontrol akses pengguna (izin) berdasarkan tanda sumber daya:

- Gunakan `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** untuk mengizinkan atau menolak tindakan pengguna pada sumber daya dengan tanda tertentu.
- Gunakan `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** untuk mengharuskan penggunaan (atau tidak mengharuskan penggunaan) tanda tertentu saat membuat permintaan API untuk membuat atau memodifikasi sumber daya yang mengizinkan tanda.
- Gunakan `aws:TagKeys`: [**`tag-key`**, …] untuk mengharuskan penggunaan (atau tidak mengharuskan penggunaan) serangkaian kunci tanda tertentu saat membuat permintaan API untuk membuat atau memodifikasi sumber daya yang mengizinkan tanda.

> **Note**
>
> Kunci dan nilai konteks syarat dalam kebijakan IAM hanya berlaku untuk tindakan AWS Directory Service tersebut di mana pengidentifikasi untuk sumber daya yang dapat ditandai adalah parameter yang diperlukan.

Mengontrol akses menggunakan tanda di Panduan Pengguna IAM memiliki informasi tambahan tentang cara menggunakan tanda. Bagian Referensi kebijakan JSON IAM dari panduan tersebut menyajikan sintaks terperinci, deskripsi, dan contoh elemen, variabel, dan logika evaluasi kebijakan JSON di IAM.

Contoh kebijakan tanda berikut memungkinkan semua panggilan `ds` selama itu berisi pasangan nilai kunci tanda "`fooKey`":"`fooValue`".

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Contoh kebijakan sumber daya berikut memungkinkan semua panggilan `ds` selama sumber daya berisi ID direktori "`d-1234567890`".

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Untuk informasi selengkapnya tentang ARN, lihat Nama Sumber Daya Amazon (ARN) dan Ruang Nama AWS Layanan.

Daftar operasi AWS Directory Service API berikut mendukung izin tingkat sumber daya berbasis tag:

- AcceptSharedDirectory
- AddIpRoutes
- AddTagsToResource
- CancelSchemaExtension
- CreateAlias
- CreateComputer
- CreateConditionalForwarder
- CreateSnapshot
- CreateLogSubscription

- CreateTrust
- DeleteConditionalForwarder
- DeleteDirectory
- DeleteLogSubscription
- DeleteSnapshot
- DeleteTrust
- DeregisterEventTopic
- DescribeConditionalForwarders
- DescribeDomainControllers
- DescribeEventTopics
- DescribeSharedDirectories
- DescribeSnapshots
- DescribeTrusts
- DisableRadius
- DisableSso
- EnableRadius
- EnableSso
- GetSnapshotLimits
- ListIpRoutes
- ListSchemaExtensions
- ListTagsForResource
- RegisterEventTopic
- RejectSharedDirectory
- RemoveIpRoutes
- RemoveTagsFromResource
- ResetUserPassword
- RestoreFromSnapshot
- ShareDirectory
- StartSchemaExtension

- UnshareDirectory
- UpdateConditionalForwarder
- UpdateNumberOfDomainControllers
- UpdateRadius
- UpdateTrust
- VerifyTrust

AWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi

Saat menyiapkan Kontrol akses dan menulis kebijakan izin yang dapat dilampirkan ke identitas IAM (kebijakan berbasis identitas), Anda dapat menggunakan tabel sebagai referensi. AWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi Setiap entri API dalam mencakup hal-hal berikut:

- Nama operasi AWS Directory Service API
- Tindakan terkait yang dapat Anda berikan izin untuk melakukan tindakan tersebut
- AWS Sumber daya yang dapat Anda berikan izin

Anda menentukan tindakan dalam bidang `Action` kebijakan, dan nilai sumber daya di dalam bidang `Resource` kebijakan. Untuk menentukan tindakan, gunakan awalan `ds:` diikuti dengan nama operasi API (misalnya, `ds:CreateDirectory`). Beberapa AWS aplikasi mungkin memerlukan penggunaan operasi AWS Directory Service API nonpublik seperti`ds:AuthorizeApplication`,,`ds:CheckAlias`, `ds:CreateIdentityPoolDirectoryds:UpdateAuthorizedApplication`, dan `ds:UnauthorizeApplication` dalam kebijakan mereka.

Beberapa AWS Directory Service API hanya dapat dipanggil melalui file AWS Management Console. Mereka bukan API publik, dalam arti mereka tidak dapat dipanggil secara terprogram, dan mereka tidak disediakan oleh SDK apa pun. Mereka menerima kredensyal pengguna. Operasi API ini meliputi`ds:DisableRoleAccess`,`ds:EnableRoleAccess`, dan`ds:UpdateDirectory`.

Anda dapat menggunakan kunci kondisi AWS global dalam AWS Directory Service kebijakan Anda untuk menyatakan kondisi. Untuk daftar lengkap AWS kunci, lihat Kunci Kondisi Global yang Tersedia di Panduan Pengguna IAM.

Topik-Topik Terkait

- Kontrol akses

Otorisasi untuk AWS aplikasi dan layanan menggunakan AWS Directory Service

Mengotorisasi AWS aplikasi pada Active Directory

AWS Directory Service memberikan izin khusus untuk aplikasi yang dipilih untuk diintegrasikan secara mulus dengan Direktori Aktif Anda saat Anda mengotorisasi aplikasi. AWS AWS aplikasi hanya diberikan akses yang diperlukan untuk kasus penggunaannya. Kumpulan izin internal yang diberikan kepada aplikasi dan administrator aplikasi setelah otorisasi disediakan di bawah ini:

> **Note**
>
> `ds:AuthorizationApplicationIzin` diperlukan untuk mengotorisasi AWS aplikasi baru Active Directory. Izin untuk tindakan ini hanya boleh diberikan kepada Administrator yang mengonfigurasi integrasi dengan Directory Service.

- Baca akses ke data pengguna, grup, unit organisasi, komputer, atau otoritas sertifikasi Active Directory di semua Unit Organisasi (OU) direktori AD Microsoft AWS Terkelola, Simple AD, AD Connector, serta domain tepercaya untuk AWS Microsoft AD Terkelola jika diizinkan oleh hubungan kepercayaan.
- Tulis akses ke pengguna, grup, keanggotaan grup, komputer, atau data otoritas sertifikasi di unit organisasi Microsoft AD yang AWS Dikelola. Tulis akses ke semua OU Simple AD.
- Otentikasi dan manajemen sesi pengguna Active Directory untuk semua jenis direktori.

Aplikasi Microsoft AD AWS Terkelola tertentu seperti Amazon RDS dan Amazon FSx terintegrasi melalui koneksi jaringan langsung ke Direktori Aktif Anda. Dalam hal ini, interaksi direktori menggunakan protokol Active Directory asli seperti LDAP dan Kerberos. Izin AWS aplikasi ini dikendalikan oleh akun pengguna direktori yang dibuat di Unit Organisasi AWS Cadangan (OU) selama otorisasi aplikasi, yang mencakup manajemen DNS dan akses penuh ke OU khusus yang dibuat untuk aplikasi. Untuk menggunakan akun ini, aplikasi memerlukan izin untuk `ds:GetAuthorizedApplicationDetails` bertindak melalui kredensil pemanggil atau peran IAM.

Untuk informasi selengkapnya tentang izin AWS Directory Service API, lihatAWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi.

Untuk informasi selengkapnya tentang mengaktifkan AWS aplikasi dan layanan untuk Microsoft AD yang AWS Dikelola, lihatAktifkan akses ke AWS aplikasi dan layanan. Untuk informasi selengkapnya tentang mengaktifkan AWS aplikasi dan layanan untuk AD Connector, lihatAktifkan akses ke AWS aplikasi dan layanan. Untuk informasi selengkapnya tentang mengaktifkan AWS aplikasi dan layanan untuk Simple AD, lihatAktifkan akses ke AWS aplikasi dan layanan.

Membatalkan otorisasi AWS aplikasi pada Active Directory

Untuk menghapus izin AWS aplikasi untuk mengakses Direktori Aktif, `ds:UnauthorizedApplication` izin diperlukan. Ikuti langkah-langkah yang disediakan oleh aplikasi untuk menonaktifkannya.

Penebangan dan pemantauan di AWS Directory Service

Sebagai praktik terbaik, pantau organisasi Anda untuk memastikan bahwa perubahan dicatat. Ini membantu Anda memastikan bahwa setiap perubahan tak terduga dapat diselidiki dan perubahan yang tidak diinginkan dapat dibatalkan. AWS Directory Service saat ini mendukung dua AWS layanan berikut sehingga Anda dapat memantau organisasi Anda dan aktivitas yang terjadi di dalamnya.

- Amazon CloudWatch - Anda dapat menggunakan CloudWatch Acara dengan jenis direktori Microsoft AD yang AWS Dikelola. Untuk informasi selengkapnya, lihat Mengaktifkan penerusan log. Selain itu, Anda dapat menggunakan CloudWatch Metrik untuk memantau kinerja pengontrol domain. Untuk informasi selengkapnya, lihat Tentukan kapan harus menambahkan pengontrol domain dengan metrik CloudWatch .
- AWS CloudTrail - Anda dapat menggunakan CloudTrail dengan semua jenis AWS Directory Service direktori. Untuk informasi selengkapnya, lihat Logging panggilan AWS Directory Service API dengan CloudTrail.

Validasi kepatuhan untuk AWS Directory Service

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

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

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

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

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

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi sumber daya AWS Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Directory Service

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat infrastruktur AWS global.

Selain infrastruktur AWS global, AWS Directory Service menawarkan kemampuan untuk mengambil snapshot manual data kapan saja untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda. Untuk informasi selengkapnya, lihat Snapshot atau pulihkan direktori Anda.

Keamanan infrastruktur di AWS Directory Service

Sebagai layanan terkelola, AWS Directory Service dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam Amazon Web Services: Ringkasan proses keamanan whitepaper.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Directory Service melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS). Kami merekomendasikan TLS 1.2 atau yang versi lebih baru. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem-sistem modern seperti Java 7 dan versi yang lebih baru mendukung mode-mode ini.

Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, lihat Standar pemrosesan informasi federal (FIPS) 140-2.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Pencegahan confused deputy lintas layanan

Masalah confused deputy adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang lebih berhak untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan pengguna utama layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan global dalam kebijakan sumber daya untuk membatasi izin yang diberikan AWS Directory Service untuk Microsoft Active Directory untuk layanan lain ke sumber daya. Jika `aws:SourceArn` nilainya tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global untuk membatasi izin. Jika Anda menggunakan kunci konteks kondisi global dan nilai `aws:SourceArn` berisi ID akun, nilai `aws:SourceAccount` dan akun dalam nilai `aws:SourceArn` harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama. Gunakan `aws:SourceArn` jika Anda hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Untuk contoh berikut, nilai `aws:SourceArn` harus berupa grup CloudWatch log.

Cara paling efektif untuk melindungi dari masalah confused deputy adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan `aws:SourceArn` dan kunci konteks kondisi `aws:SourceAccount` global di Microsoft AD yang AWS Dikelola untuk mencegah masalah deputi yang membingungkan.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
```

```
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
    "Resource": [
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Untuk contoh berikut, nilai `aws:SourceArn` harus menjadi topik SNS di akun Anda. Misalnya, Anda dapat menggunakan sesuatu seperti `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` di mana “ap-tenggara 1" adalah wilayah Anda, “123456789012" adalah id pelanggan Anda dan" _d-966739499f” adalah nama topik Amazon SNS yang Anda buat. DirectoryMonitoring

Cara paling efektif untuk melindungi dari masalah confused deputy adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan `aws:SourceArn` dan kunci konteks kondisi `aws:SourceAccount` global di Microsoft AD yang AWS Dikelola untuk mencegah masalah deputi yang membingungkan.

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

```
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": ["SNS:GetTopicAttributes",
     "SNS:SetTopicAttributes",
        "SNS:AddPermission",
     "SNS:RemovePermission",
     "SNS:DeleteTopic",
     "SNS:Subscribe",
     "SNS:ListSubscriptionsByTopic",
     "SNS:Publish"],
    "Resource": [
      "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Contoh berikut menunjukkan kebijakan kepercayaan IAM untuk peran yang telah didelegasikan akses konsol. Nilai `aws:SourceArn` harus berupa sumber daya direktori di akun Anda. Untuk informasi selengkapnya, lihat Jenis sumber daya yang ditentukan oleh AWS Directory Service. Misalnya, Anda dapat menggunakan `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890` di `123456789012` mana ID pelanggan Anda dan `d-1234567890` ID direktori Anda.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
```

```
    "Action": [
                "sts:AssumeRole"
            ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Akses AWS Directory Service API menggunakan titik akhir antarmuka - AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC dan AWS Directory Service API Anda. Anda dapat mengakses AWS Directory Service API seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk AWS Directory Service mengakses API.

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 pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan. AWS Directory Service

Untuk informasi selengkapnya, lihat Akses Layanan AWS melalui AWS PrivateLink di AWS PrivateLink Panduan.

Pertimbangan untuk AWS Directory Service

Sebelum menyiapkan titik akhir antarmuka untuk titik akhir AWS Directory Service API, tinjau Pertimbangan dalam Panduan.AWS PrivateLink

AWS Directory Service mendukung panggilan ke semua tindakan API-nya melalui titik akhir antarmuka.

Ketersediaan

AWS Directory Service mendukung titik akhir VPC sebagai berikut: Wilayah AWS

- AS Timur (Virginia Utara)
- AWS GovCloud (AS-Barat)
- AWS GovCloud (AS-Timur)

Buat titik akhir antarmuka untuk AWS Directory Service

Anda dapat membuat titik akhir antarmuka untuk AWS Directory Service API menggunakan konsol VPC Amazon atau AWS Command Line Interface ().AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir antarmuka untuk AWS Directory Service API menggunakan nama layanan berikut:

```
com.amazonaws.region.ds
```

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 Directory Service API melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan ke AWS Directory Service API 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.
- Sumber daya untuk melakukan tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh: Kebijakan titik akhir VPC untuk tindakan API AWS Directory Service

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke AWS Directory Service tindakan

yang tercantum untuk semua prinsip di semua sumber daya. Ganti *action-1*, *action-2*, dan *action-3* dengan izin yang diperlukan untuk AWS Directory Service API yang ingin Anda sertakan dalam kebijakan Anda. Untuk daftar lengkap, lihat AWS Directory Service Izin API: Referensi tindakan, sumber daya, dan kondisi.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:action-1",
            "ds:action-2",
            "ds:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Perjanjian tingkat layanan untuk AWS Directory Service

AWS Directory Service adalah layanan yang sangat tersedia, dan dibangun di infrastruktur yang dikelola AWS. didukung oleh perjanjian tingkat layanan yang menentukan kebijakan ketersediaan layanan kami.

Untuk informasi selengkapnya, lihat Perjanjian tingkat layanan untuk AWS Directory Service.

Ketersediaan wilayah untuk AWS Directory Service

Tabel berikut menyediakan daftar yang menjelaskan titik akhir khusus Region yang didukung oleh jenis direktori.

Nama Region	Wilayah	Titik Akhir	Protokol	AWS Microsof AD yang dikelola	AD Connect	Simple AD
US East (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	Y	Y	Tidak
US East (Northern Virginia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	Y	Y	Ya
US West (Northern California)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	Y	Y	Tidak
AS Barat (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	Y	Y	Ya
Afrika (Cape Town)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	Y	Y	Tidak
Asia Pasifik	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	Y	Y	Tidak

Nama Region	Wilayah	Titik Akhir	Protokol	AWS Microsof AD yang dikelola	AD Connect	Simple AD
(Hong Kong)						
Asia Pasifik (Mumbai	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	Y	Y	Tidak
Asia Pasifik (Hyderab d)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	Y	Y	Tidak
Asia Pacific (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	Y	Y	Tidak
Asia Pasifik (Seoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	Y	Y	Tidak
Asia Pasifik (Singapu a)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	Y	Y	Ya
Asia Pasifik (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	Y	Y	Ya
Asia Pasifik (Jakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	Y	Y	Tidak

Nama Region	Wilayah	Titik Akhir	Protokol	AWS Microsof AD yang dikelola	AD Connect	Simple AD
Asia Pacific (Melbour e)	ap-southe ast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 Y	 Y	 Tidak
Asia Pasifik (Tokyo)	ap-northe ast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 Y	 Y	 Ya
Kanada (Pusat)	ca-centra l-1	ds.ca-central-1.amazonaws.com	HTTPS	 Y	 Y	 Tidak
Kanada Barat (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 Y	 Y	 Tidak
Tiongkok (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 Y	 Y	 Tidak
Tiongkok (Ningxia)	cn-northw est-1	ds.cn-northwest-1.amazonaws .com.cn	HTTPS	 Y	 Y	 Tidak
Eropa (Frankfu t)	eu-centra l-1	ds.eu-central-1.amazonaws.com	HTTPS	 Y	 Y	 Tidak
Europe (Zurich)	eu-centra l-2	ds.eu-central-2.amazonaws.com	HTTPS	 Y	 Y	 Tidak

Nama Region	Wilayah	Titik Akhir	Protokol	AWS Microsoft AD yang dikelola	AD Connector	Simple AD
Eropa (Irlandia)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	Ya	Ya	Ya
Eropa (London)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	Ya	Ya	Tidak
Eropa (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	Ya	Ya	Tidak
Eropa (Stockholm)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	Ya	Ya	Tidak
Eropa (Milan)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	Ya	Ya	Tidak
Eropa (Spanyol	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	Ya	Ya	Tidak
Israel (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	Ya	Ya	Tidak
Timur Tengah (Bahrain)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	Ya	Ya	Tidak

Nama Region	Wilayah	Titik Akhir	Protokol	AWS Microsof AD yang dikelola	AD Connect	Simple AD
Timur Tengah (UAE)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	Y	Y	Tidak
Amerika Selatan (Sao Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	Y	Y	Tidak
AWS GovClou (AS-Barat)	us-gov-west-1	ds. us-gov-west-1.amazonaws.com	HTTPS	Y	Y	Tidak
AWS GovClou (AS-Timur)	us-gov-east-1	ds. us-gov-east-1.amazonaws.com	HTTPS	Y	Y	Tidak

Untuk informasi tentang penggunaan AWS Directory Service di Wilayah AWS GovCloud (AS-Barat) dan Wilayah AWS GovCloud (AS-Timur), lihat Titik akhir layanan.

Untuk informasi tentang penggunaan AWS Directory Service di Wilayah Beijing dan Ningxia, lihat Titik Akhir dan ARN untuk Amazon Web Services di Tiongkok.

Kompabilitas peramban

AWS aplikasi dan layanan seperti WorkSpaces, Amazon, Amazon Connect WorkMail, Amazon Chime, Amazon WorkDocs, dan AWS IAM Identity Center semuanya memerlukan kredensi masuk yang valid dari browser yang kompatibel sebelum Anda dapat mengaksesnya. Tabel berikut menjelaskan hanya peramban dan versi peramban yang kompatibel untuk masuk.

Peramban	Versi	Kompatibilitas
Microsoft Internet Explorer	Desktop IE versi 7 dan di bawahnya	Tidak kompatibel
	Desktop IE versi 8, 9, dan 10	Kompatibel hanya saat menjalankan Windows 7 atau yang lebih baru dan TLS 1.1 diaktifkan. Untuk informasi selengkapnya, lihat Apa itu TLS?.
	Desktop IE versi 11 dan di atasnya	Kompatibel
	Mobile IE versi 10 dan di bawahnya	Tidak kompatibel
	Mobile IE versi 11 dan di atasnya	Kompatibel
Microsoft Edge	Semua versi	Kompatibel
Mozilla Firefox	Firefox 23 dan di bawahnya	Tidak kompatibel
	Firefox 24 hingga 26	Kompatibel, tapi tidak secara default.
	Firefox 27 dan di atasnya	Kompatibel
Google Chrome	Google Chrome 21 dan di bawahnya	Tidak kompatibel
	Google Chrome 22 hingga 37	Kompatibel, tapi tidak secara default.
	Google Chrome 38 dan di atasnya	Kompatibel

Peramban	Versi	Kompatibilitas
Apple Safari	Safari Desktop versi 6 dan ke atasnya untuk OS X 10.8 (Mountain Lion) dan ke bawahnya	Tidak kompatibel
	Safari Desktop versi 7 dan yang lebih tinggi untuk OS X 10.9 (Mavericks) dan yang lebih tinggi	Kompatibel
	Mobile Safari untuk iOS 4 dan ke bawahnya	Tidak kompatibel
	Mobile Safari versi 5 dan yang lebih tinggi untuk iOS 5 dan yang lebih tinggi	Kompatibel

Setelah Anda memverifikasi bahwa Anda menggunakan versi peramban yang didukung, sebaiknya Anda juga meninjau bagian di bawah ini untuk memverifikasi bahwa peramban Anda telah dikonfigurasi untuk menggunakan pengaturan Keamanan Lapisan Pengangkutan (TLS) yang diperlukan oleh AWS.

Apa itu TLS?

TLS adalah peramban web protokol dan aplikasi lain yang digunakan untuk bertukar data secara aman melewati jaringan. TLS memastikan bahwa hubungan ke titik akhir jauh adalah titik akhir yang dimaksudkan melalui enkripsi dan verifikasi identitas titik akhir. Versi TLS, hingga saat ini, adalah TLS 1.0, 1.1, 1.2 dan 1.3.

Versi TLS mana yang didukung oleh IAM Identity Center

AWS aplikasi dan layanan mendukung TLS 1.1, 1.2 dan 1.3 untuk login aman. Mulai 30 Oktober 2019, TLS 1.0 tidak lagi didukung, jadi penting agar semua peramban dikonfigurasi untuk mendukung TLS 1.1 atau yang di atasnya. Ini berarti, Anda tidak akan dapat masuk ke aplikasi dan layanan AWS jika Anda mengaksesnya saat TLS 1.0 diaktifkan. Untuk bantuan dalam membuat perubahan ini, kontak admin Anda.

Bagaimana cara mengaktifkan versi TLS yang didukung di peramban saya

Hal ini tergantung pada peramban Anda. Biasanya Anda dapat menemukan pengaturan ini di bawah area pengaturan lanjutan di pengaturan peramban Anda. Misalnya, di Internet Explorer Anda akan menemukan berbagai pilihan TLS di bawah Properti internet, tab Advanced, dan kemudian di bawah bagian Keamanan. Periksa situs web Bantuan produsen peramban Anda untuk petunjuk tertentu.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilisan terakhir dari AWS Directory Service Panduan Administrator.

Perubahan	Deskripsi	Tanggal
Pengaturan otentikasi berbasis sertifikat	Menambahkan konten tentang dua pengaturan keamanan baru untuk Microsoft AD yang AWS Dikelola.	11 April 2023
AWS PrivateLink	Menambahkan konten tentang AWS PrivateLink.	31 Maret 2023
Titik Akhir VPC AD Sederhana	Menambahkan konten tentang titik akhir VPC mana yang tidak boleh dikonfigurasi.	25 Agustus 2021
Titik Akhir VPC Konektor AD	Menambahkan konten tentang titik akhir VPC mana yang tidak boleh dikonfigurasi.	25 Agustus 2021
Dukungan kartu pintar	Menambahkan konten tentang dukungan untuk kartu pintar dan Amazon WorkSpace s Application Manager di Wilayah AWS GovCloud (AS-Barat)	1 Desember 2020
Reset kata sandi	Menambahkan konten tentang cara mengatur ulang kata sandi pengguna menggunakan AWS Management Console, Windows PowerShell dan AWS CLI.	2 Januari 2019

Berbagi direktori	Menambahkan konten tentang cara menggunakan berbagi direktori dengan Microsoft AD yang AWS Dikelola.	25 September 2018
Konten yang dimigrasi ke Panduan Pengembang Amazon Cloud Directory baru	Memindahkan konten Amazon Cloud Directory dari panduan ini ke Panduan Pengembang Amazon Cloud Directory yang baru.	21 Juni 2018
Perombakan lengkap panduan admin TOC	Menata ulang konten untuk lebih langsung memenuhi kebutuhan pelanggan. Juga menambahkan konten baru jika diperlukan.	5 April 2018
AWS kelompok yang didelegasikan	Menambahkan daftar grup AWS yang didelegasikan yang dapat ditetapkan ke pengguna lokal.	8 Maret 2018
Kebijakan kata sandi berbutir halus	Menambahkan konten tentang kebijakan kata sandi baru.	5 Juli 2017
Pengontrol domain tambahan	Menambahkan konten tentang cara menambahkan lebih banyak pengontrol domain ke direktori Anda di Microsoft AD yang AWS Dikelola.	30 Juni 2017
Tutorial	Menambahkan tutorial baru untuk menguji lingkungan lab Microsoft AD AWS Terkelola.	21 Juni 2017

MFA dengan AWS Microsoft AD yang Dikelola	Menambahkan konten tentang penggunaan MFA dengan AWS Microsoft AD yang Dikelola.	13 Februari 2017
Amazon Cloud Directory	Menambahkan konten tentang jenis direktori baru.	26 Januari 2017
Ekstensi skema	Menambahkan konten tentang ekstensi skema dengan AWS Directory Service untuk Microsoft Active Directory.	14 November 2016
Reorganisasi besar dari Panduan AWS Directory Service Administrator	Menata ulang konten untuk lebih langsung memenuhi kebutuhan pelanggan.	14 November 2016
Pemberitahuan SNS	Menambahkan konten tentang notifikasi SNS.	25 Februari 2016
Otorisasi dan otentikasi	Menambahkan konten tentang cara menggunakan IAM dengan AWS Directory Service.	25 Februari 2016
AWS Microsoft AD yang dikelola	Menambahkan konten tentang Microsoft AD yang AWS Dikelola dan panduan gabungan ke dalam satu panduan.	17 November 2015
Izinkan instance Linux untuk digabungkan ke direktori Simple AD	Menambahkan konten tentang cara menggabungkan instance Linux ke direktori Simple AD.	23 Juli 2015
Pemisahan panduan	Pisahkan Panduan AWS Directory Service Administrasi menjadi panduan terpisah.	14 Juli 2015

Dukungan masuk tunggal	Menambahkan konten tentang dukungan untuk sistem masuk tunggal.	31 Maret 2015
Panduan baru	Ini adalah rilisan pertama dari AWS Directory Service Panduan Administrasi.	21 Oktober 2014

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