



Panduan Pengguna

Studio Penelitian dan Teknik



Studio Penelitian dan Teknik: Panduan Pengguna

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Gambaran Umum	1
Fitur dan manfaat	1
Konsep dan definisi	3
Gambaran umum arsitektur	5
Diagram arsitektur	5
AWS layanan dalam produk ini	6
Lingkungan demo	10
Buat tumpukan demo satu klik	10
Prasyarat	10
Buat sumber daya dan parameter masukan	11
Langkah-langkah penyebaran pasca	12
Rencanakan penyebaran Anda	14
Biaya	14
Keamanan	14
Peran IAM	15
Grup keamanan	15
Enkripsi data	15
Pertimbangan keamanan produk	16
Kuota	19
Kuota untuk AWS layanan dalam produk ini	19
AWS CloudFormation kuota	20
Perencanaan ketahanan	20
Didukung Wilayah AWS	20
Menyebarkan produk	22
Prasyarat	22
Buat Akun AWS dengan pengguna administratif	23
Buat key pair Amazon EC2 SSH	23
Tingkatkan kuota layanan	23
Buat domain publik (opsional)	24
Buat domain (GovCloud hanya)	24
Menyediakan sumber daya eksternal	25
Konfigurasikan LDAPS di lingkungan Anda (opsional)	26
Konfigurasikan VPC pribadi (opsional)	27
Buat sumber daya eksternal	39

Langkah 1: Luncurkan produk	45
Langkah 2: Masuk untuk pertama kalinya	53
Perbarui produk	54
Pembaruan versi utama	54
Pembaruan versi minor	54
Copot pemasangan produk	56
Menggunakan AWS Management Console	56
Menggunakan AWS Command Line Interface	56
Menghapus shared-storage-security-group	56
Menghapus bucket Amazon S3	57
Panduan konfigurasi	58
Manajemen identitas	58
Penyiapan identitas Amazon Cognito	59
Sinkronisasi Direktori Aktif	61
Menyiapkan SSO dengan IAM Identity Center	63
Mengkonfigurasi penyedia identitas Anda untuk SSO	66
Mengatur kata sandi untuk pengguna	73
Membuat subdomain	73
Buat sertifikat ACM	74
CloudWatch Log Amazon	75
Menetapkan batas izin khusus	76
Konfigurasi RES-Ready AMIs	80
Siapkan peran IAM untuk mengakses lingkungan RES	81
Buat komponen EC2 Image Builder	83
Siapkan resep EC2 Image Builder Anda	87
Konfigurasi infrastruktur EC2 Image Builder	89
Konfigurasi pipa gambar Image Builder	90
Jalankan pipa gambar Image Builder	91
Daftarkan tumpukan perangkat lunak baru di RES	91
Panduan administrator	92
Manajemen rahasia	92
Pemantauan dan pengendalian biaya	95
Manajemen sesi	97
Dasbor	97
Sesi	98
Tumpukan Perangkat Lunak () AMIs	99

Debugging	100
Pengaturan desktop	100
Pengelolaan lingkungan	101
Status lingkungan	102
Pengaturan lingkungan	102
Pengguna	102
Grup	103
Proyek	103
Kebijakan izin	107
Sistem File	114
Manajemen snapshot	115
Bucket Amazon S3	120
Gunakan produk	134
Akses SSH	134
Desktop virtual	134
Luncurkan desktop baru	135
Akses desktop Anda	135
Kontrol status desktop Anda	136
Memodifikasi desktop virtual	136
Ambil informasi sesi	137
Jadwalkan desktop virtual	137
VDI autostop	138
Desktop bersama	138
Bagikan desktop	139
Mengakses desktop bersama	139
Browser file	139
Unggah file	140
Hapus berkas	140
Kelola favorit	140
Mengedit file	141
Transfer file	141
Pemecahan Masalah	142
Debugging dan Pemantauan Umum	145
Sumber informasi log dan peristiwa yang berguna	145
Penampilan EC2 Konsol Amazon Khas	149
Debugging Windows DCV	151

Temukan Informasi Versi Amazon DCV	151
Masalah RunBooks	152
Masalah instalasi	154
Masalah manajemen identitas	162
Penyimpanan	167
Snapshot	170
Infrastruktur	171
Meluncurkan Desktop Virtual	172
Komponen Desktop Virtual	176
Penghapusan Env	181
Lingkungan demo	186
Masalah yang Diketahui	188
Masalah yang Diketahui 2024.x	189
Pemberitahuan	207
Revisi	208
.....	CCX

Gambaran Umum

Important

Versi Panduan Pengguna ini mencakup rilis 2024.12 Studio Penelitian dan Teknik di AWS. Untuk versi saat ini, lihat [Studio Riset dan Teknik di Panduan AWS Pengguna](#).

Research and Engineering Studio (RES) adalah produk open source yang AWS didukung yang memungkinkan administrator TI menyediakan portal web bagi para ilmuwan dan insinyur untuk menjalankan beban kerja komputasi teknis. AWS RES menyediakan satu panel kaca bagi pengguna untuk meluncurkan desktop virtual yang aman untuk melakukan penelitian ilmiah, desain produk, simulasi teknik, atau beban kerja analisis data. Pengguna dapat terhubung ke portal RES menggunakan kredensial perusahaan yang ada dan bekerja pada proyek individu atau kolaboratif.

Administrator dapat membuat ruang kolaborasi virtual yang disebut proyek untuk sekumpulan pengguna tertentu untuk mengakses sumber daya bersama dan berkolaborasi. Administrator dapat membangun tumpukan perangkat lunak aplikasi mereka sendiri (menggunakan [Amazon Machine Images](#) atau AMIs) dan memungkinkan pengguna RES untuk meluncurkan desktop virtual Windows atau Linux, dan mengaktifkan akses ke data proyek melalui sistem file bersama. Administrator dapat menetapkan tumpukan perangkat lunak dan sistem file dan membatasi akses hanya untuk pengguna proyek tersebut. Administrator dapat menggunakan telemetri bawaan untuk memantau penggunaan lingkungan dan memecahkan masalah pengguna. Mereka juga dapat menetapkan anggaran untuk proyek individu untuk mencegah konsumsi sumber daya yang berlebihan. Karena produk ini open source, pelanggan juga dapat menyesuaikan pengalaman pengguna portal RES agar sesuai dengan kebutuhan mereka sendiri.

RES tersedia tanpa biaya tambahan, dan Anda hanya membayar untuk AWS sumber daya yang dibutuhkan untuk menjalankan aplikasi Anda.

Panduan ini memberikan gambaran umum tentang Research and Engineering Studio on AWS, arsitektur referensi dan komponennya, pertimbangan untuk merencanakan penyebaran, dan langkah-langkah konfigurasi untuk menerapkan RES ke Amazon Web Services (AWS Cloud).

Fitur dan manfaat

Research and Engineering Studio on AWS menyediakan fitur-fitur berikut:

Antarmuka pengguna berbasis web

RES menyediakan portal berbasis web yang dapat digunakan administrator, peneliti, dan insinyur untuk mengakses dan mengelola ruang kerja penelitian dan teknik mereka. Ilmuwan dan insinyur tidak perlu memiliki keahlian cloud Akun AWS atau cloud untuk menggunakan RES.

Konfigurasi berbasis proyek

Gunakan proyek untuk menentukan izin akses, mengalokasikan sumber daya, dan mengelola anggaran untuk serangkaian tugas atau aktivitas. Tetapkan tumpukan perangkat lunak tertentu (sistem operasi dan aplikasi yang disetujui) dan sumber daya penyimpanan untuk proyek untuk konsistensi dan kepatuhan. Memantau dan mengelola pengeluaran berdasarkan per proyek.

Alat kolaborasi

Para ilmuwan dan insinyur dapat mengundang anggota lain dari proyek mereka untuk berkolaborasi dengan mereka, menetapkan tingkat izin yang mereka inginkan dari rekan-rekan tersebut. Orang-orang tersebut dapat masuk ke RES untuk terhubung ke desktop tersebut.

Integrasi dengan infrastruktur manajemen identitas yang ada

Integrasikan dengan manajemen identitas dan infrastruktur layanan direktori yang ada untuk mengaktifkan koneksi ke portal RES dengan identitas perusahaan pengguna yang ada dan menetapkan izin untuk proyek menggunakan keanggotaan pengguna dan grup yang ada.

Penyimpanan persisten dan akses ke data bersama

Untuk memberi pengguna akses ke data bersama di seluruh sesi desktop virtual, sambungkan ke sistem file yang ada di dalam RES. Layanan penyimpanan yang didukung termasuk Amazon Elastic File System untuk desktop Linux dan Amazon FSx untuk NetApp ONTAP untuk desktop Windows dan Linux.

Pemantauan dan pelaporan

Gunakan dasbor analitik untuk memantau penggunaan sumber daya untuk jenis instans, tumpukan perangkat lunak, dan jenis sistem operasi. Dasbor juga menyediakan rincian penggunaan sumber daya oleh proyek untuk pelaporan.

Anggaran dan manajemen biaya

Tautkan AWS Budgets ke proyek RES Anda untuk memantau biaya untuk setiap proyek. Jika Anda melebihi anggaran Anda, Anda dapat membatasi peluncuran sesi VDI.

Konsep dan definisi

Bagian ini menjelaskan konsep-konsep kunci dan mendefinisikan terminologi khusus untuk Research and Engineering Studio pada: AWS

Browser file

Browser file adalah bagian dari antarmuka pengguna RES di mana pengguna yang saat ini masuk dapat melihat sistem file mereka.

Sistem file

Sistem file bertindak sebagai wadah untuk data proyek (sering disebut sebagai dataset). Ini menyediakan solusi penyimpanan dalam batas-batas proyek dan meningkatkan kolaborasi dan kontrol akses data.

Administrator global

Delegasi administratif dengan akses ke sumber daya RES yang dibagikan di seluruh lingkungan RES. Cakupan dan izin mencakup beberapa proyek. Mereka dapat membuat atau memodifikasi proyek dan menetapkan pemilik proyek. Mereka dapat mendelegasikan atau menetapkan izin kepada pemilik proyek dan anggota proyek. Terkadang orang yang sama bertindak sebagai administrator RES tergantung pada ukuran organisasi.

Proyek

Proyek adalah partisi logis dalam aplikasi yang berfungsi sebagai batas yang berbeda untuk data dan sumber daya komputasi; ini memastikan tata kelola atas aliran data dan mencegah berbagi data dan host VDI di seluruh proyek.

Izin berbasis proyek

Izin berbasis proyek menggambarkan partisi logis dari kedua data dan host VDI dalam sistem di mana beberapa proyek dapat ada. Akses pengguna ke data dan host VDI dalam proyek ditentukan oleh peran terkait mereka. Seorang pengguna harus diberi akses (atau keanggotaan proyek) untuk setiap proyek yang mereka perlukan aksesnya. Jika tidak, pengguna tidak dapat mengakses data proyek dan VDIs ketika mereka belum diberikan keanggotaan.

Anggota proyek

Pengguna akhir sumber daya RES (VDI, penyimpanan, dll). Cakupan dan izin dibatasi untuk proyek yang ditugaskan untuk mereka. Mereka tidak dapat mendelegasikan atau menetapkan izin apa pun.

Pemilik proyek

Delegasi administratif dengan akses ke, dan kepemilikan atas, proyek tertentu. Cakupan dan izin dibatasi untuk proyek yang mereka miliki. Mereka dapat menetapkan izin untuk anggota proyek dalam proyek yang mereka miliki.

Tumpukan perangkat lunak

Tumpukan perangkat lunak adalah [Amazon Machine Images \(AMI\)](#) dengan metadata khusus RES berdasarkan sistem operasi apa pun yang telah dipilih pengguna untuk disediakan untuk host VDI mereka.

Tuan rumah VDI

Host virtual desktop instance (VDI) memungkinkan anggota proyek mengakses data spesifik proyek dan lingkungan komputasi, memastikan ruang kerja yang aman dan terisolasi.

Untuk referensi umum AWS istilah, lihat [AWS glosarium](#) di Referensi AWS Umum.

Gambaran umum arsitektur

Bagian ini menyediakan diagram arsitektur untuk komponen yang digunakan dengan produk ini.

Diagram arsitektur

Menyebarkan produk ini dengan parameter default menyebarkan komponen berikut di Anda. Akun AWS

Gambar 1: Studio Penelitian dan Teknik tentang AWS arsitektur

Note

AWS CloudFormation sumber daya dibuat dari AWS Cloud Development Kit (AWS CDK) konstruksi.

Alur proses tingkat tinggi untuk komponen produk yang digunakan dengan AWS CloudFormation template adalah sebagai berikut:

1. RES menginstal komponen untuk portal web serta:
 - a. Komponen Rekayasa Virtual Desktop (eVDI) untuk beban kerja interaktif
 - b. Komponen metrik

Amazon CloudWatch menerima metrik dari komponen eVDI.
 - c. Komponen Host Bastion

Administrator dapat menggunakan SSH untuk terhubung ke komponen host bastion untuk mengelola infrastruktur yang mendasarinya.
2. RES menginstal komponen dalam subnet pribadi di belakang gateway NAT. Administrator mengakses subnet pribadi melalui Application Load Balancer (ALB) atau komponen Bastion Host.
3. Amazon DynamoDB menyimpan konfigurasi lingkungan.
4. AWS Certificate Manager (ACM) menghasilkan dan menyimpan sertifikat publik untuk Application Load Balancer (ALB).

Note

Sebaiknya gunakan AWS Certificate Manager untuk menghasilkan sertifikat tepercaya untuk domain Anda.

5. Amazon Elastic File System (EFS) menghosting sistem /home file default yang dipasang pada semua host infrastruktur yang berlaku dan sesi eVDi Linux.
6. RES menggunakan Amazon Cognito untuk membuat pengguna bootstrap awal yang disebut 'clusteradmin' di dalam dan mengirimkan kredensyal sementara ke alamat email yang disediakan selama instalasi. 'Clusteradmin' harus mengubah kata sandi saat pertama kali masuk.
7. Amazon Cognito terintegrasi dengan Direktori Aktif organisasi Anda dan identitas pengguna untuk pengelolaan izin.
8. Zona keamanan memungkinkan administrator untuk membatasi akses ke komponen tertentu dalam produk berdasarkan izin.

AWS layanan dalam produk ini

AWS layanan	Tipe	Deskripsi
Amazon Elastic Compute Cloud	Core	Menyediakan layanan komputasi yang mendasari untuk membuat desktop virtual dengan sistem operasi dan tumpukan perangkat lunak pilihan mereka.
Elastic Load Balancing	Core	Host Bastion, cluster-manager, dan VDI dibuat di grup Auto Scaling di belakang load balancer. ELB menyeimbangkan lalu lintas dari portal web di seluruh host RES.
Amazon Virtual Private Cloud	Core	Semua komponen produk inti dibuat dalam VPC Anda.

AWS layanan	Tipe	Deskripsi
Amazon Cognito	Core	Mengelola identitas pengguna dan otentikasi. Pengguna Active Directory dipetakan ke pengguna dan grup Amazon Cognito untuk mengautentikasi tingkat akses.
Sistem File Elastis Amazon	Core	Menyediakan sistem /home file untuk browser file dan host VDI, serta sistem file eksternal bersama.
Amazon DynamoDB	Core	Menyimpan data konfigurasi seperti pengguna, grup, proyek, sistem file, dan pengaturan komponen.
AWS Systems Manager	Core	Menyimpan dokumen untuk melakukan perintah untuk manajemen sesi VDI.
AWS Lambda	Core	Mendukung fungsionalitas produk seperti memperbarui pengaturan dalam tabel DynamoDB, memulai alur kerja sinkronisasi Active Directory, dan memperbarui daftar awalan.
Amazon CloudWatch	Mendukung	Menyediakan metrik dan log aktivitas untuk semua EC2 host Amazon dan fungsi Lambda.

AWS layanan	Tipe	Deskripsi
<u>Layanan Penyimpanan Sederhana Amazon</u>	Mendukung	Menyimpan binari aplikasi untuk bootstrap dan konfigurasi host.
<u>AWS Key Management Service</u>	Mendukung	Digunakan untuk enkripsi saat istirahat dengan antrian Amazon SQS, tabel DynamoDB, dan topik Amazon SNS.
<u>AWS Secrets Manager</u>	Mendukung	Menyimpan kredensi akun layanan di Active Directory dan sertifikat yang ditandatangani sendiri untuk VDI
<u>AWS CloudFormation</u>	Mendukung	Menyediakan mekanisme penyebaran untuk produk.
<u>AWS Identity and Access Management</u>	Mendukung	Membatasi tingkat akses untuk host.
<u>Rute Amazon 53</u>	Mendukung	Membuat zona host pribadi untuk menyelesaikan penyeimbang beban internal dan nama domain host bastion.
<u>Amazon Simple Queue Service</u>	Mendukung	Membuat antrian tugas untuk mendukung eksekusi asinkron.
<u>Layanan Pemberitahuan Sederhana Amazon</u>	Mendukung	Mendukung model publisasi-pelanggan antara komponen VDI seperti controller dan host.

AWS layanan	Tipe	Deskripsi
AWS Fargate	Mendukung	Menginstal, memperbarui, dan menghapus lingkungan menggunakan tugas Fargate.
Gerbang FSx File Amazon	Opsional	Menyediakan sistem file bersama eksternal.
Amazon FSx untuk NetApp ONTAP	Opsional	Menyediakan sistem file bersama eksternal.
AWS Certificate Manager	Opsional	Menghasilkan sertifikat tepercaya untuk domain kustom Anda.
AWS Backup	Opsional	Menawarkan kemampuan cadangan untuk EC2 host Amazon, sistem file, dan DynamoDB.

Buat lingkungan demo

Ikuti langkah-langkah di bagian ini untuk mencoba Research and Engineering Studio di AWS. Demo ini menyebarkan lingkungan non-produksi dengan serangkaian parameter minimal menggunakan [Research and Engineering Studio pada template tumpukan lingkungan AWS demo](#). Ini menggunakan server Keycloak untuk SSO.

Perhatikan bahwa setelah Anda menyebarkan tumpukan, Anda harus mengikuti di [Langkah-langkah penyebaran pasca](#) bawah ini untuk mengatur pengguna di lingkungan sebelum Anda masuk.

Buat tumpukan demo satu klik

AWS CloudFormation Tumpukan ini menciptakan semua komponen yang dibutuhkan oleh Research and Engineering Studio.

Waktu untuk menyebarkan: ~ 90 menit

Prasyarat

Topik

- [Buat Akun AWS dengan pengguna administratif](#)
- [Buat key pair Amazon EC2 SSH](#)
- [Tingkatkan kuota layanan](#)

Buat Akun AWS dengan pengguna administratif

Anda harus memiliki Akun AWS dengan pengguna administratif:

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

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

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

Buat key pair Amazon EC2 SSH

Jika Anda tidak memiliki Amazon EC2 SSH key pair, Anda harus membuatnya. Untuk informasi selengkapnya, lihat [Membuat key pair menggunakan Amazon EC2](#) di Panduan EC2 Pengguna Amazon.

Tingkatkan kuota layanan

Kami merekomendasikan untuk [meningkatkan kuota layanan](#) untuk:

- [Amazon VPC](#)
 - Meningkatkan kuota alamat IP Elastic per gateway NAT dari lima menjadi delapan
 - Tingkatkan gateway NAT per Availability Zone dari lima menjadi sepuluh
- [Amazon EC2](#)
 - Tingkatkan EC2 -VPC Elastic IPs dari lima menjadi sepuluh

AWS Akun Anda memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan. Untuk informasi selengkapnya, lihat [the section called “Kuota untuk AWS layanan dalam produk ini”](#).

Buat sumber daya dan parameter masukan

1. Masuk ke AWS Management Console dan buka AWS CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.

Note

Pastikan Anda berada di akun administrator Anda.

2. [Luncurkan template](#) di konsol.
3. Di bawah Parameter, tinjau parameter untuk templat produk ini dan modifikasi sesuai kebutuhan.

Parameter	Default	Deskripsi
EnvironmentName	<i><res-demo></i>	Nama unik yang diberikan ke lingkungan RES Anda

Parameter	Default	Deskripsi
		dimulai dengan res-, tidak lebih dari 11 karakter, dan tidak ada huruf kapital.
AdministratorEmail		Alamat email untuk pengguna yang menyelesaikan penyiapan produk. Pengguna ini juga berfungsi sebagai pengguna break-glass jika ada tanda tunggal Active Directory pada kegagalan integrasi.
KeyPair		Key pair digunakan untuk terhubung ke host infrastruktur.
Klien IPCidr	<0.0.0.0/0>	Filter alamat IP yang membatasi koneksi ke sistem. Anda dapat memperbarui ClientIpCidr setelah penerapan.
InboundPrefixList		(Opsional) Berikan daftar awalan terkelola agar IPs diizinkan mengakses UI web dan SSH secara langsung ke host bastion.

4. Pilih Buat tumpukan.

Langkah-langkah penyebaran pasca

1. Anda sekarang dapat masuk ke lingkungan demo menggunakan pengguna clusteradmin dan kata sandi sementara yang dikirim ke email administrator yang Anda masukkan selama pengaturan. Anda diminta untuk membuat kata sandi baru pada login pertama Anda.

2. Jika Anda ingin menggunakan fitur “Masuk dengan SSO organisasi”, Anda harus terlebih dahulu mengatur ulang kata sandi untuk setiap pengguna yang ingin Anda masuki. Anda dapat mengatur ulang kata sandi pengguna dari AWS Directory Service. Tumpukan demo menciptakan empat pengguna dengan nama pengguna yang dapat Anda gunakan: admin1, user1, admin2, dan user2.
 - a. Buka konsol Directory Service.
 - b. Pilih Id Direktori untuk lingkungan Anda. Anda bisa mendapatkan Id Direktori dari output `<StackName>*DirectoryService*` tumpukan.
 - c. Dari menu dropdown Action kanan atas, pilih Reset password pengguna.
 - d. Untuk semua pengguna yang ingin Anda gunakan, masukkan nama pengguna, ketik kata sandi baru yang Anda inginkan dan kemudian pilih Atur Ulang Kata Sandi.
3. Setelah Anda mengatur ulang kata sandi pengguna, lanjutkan ke halaman masuk masuk tunggal untuk mengakses lingkungan.

Penerapan Anda sekarang siap. Gunakan yang EnvironmentUrl Anda terima di email untuk mengakses UI, atau Anda juga bisa mendapatkan URL yang sama dari output tumpukan yang diterapkan. Anda sekarang dapat masuk ke lingkungan Research and Engineering Studio dengan pengguna dan kata sandi yang Anda atur ulang kata sandi di Active Directory.

Rencanakan penyebaran Anda

Bagian ini berisi informasi tentang biaya, keamanan, wilayah yang didukung, dan kuota yang dapat membantu Anda merencanakan penyebaran Studio Riset dan Teknik. AWS

Biaya

Research and Engineering Studio on AWS tersedia tanpa biaya tambahan, dan Anda hanya membayar AWS sumber daya yang dibutuhkan untuk menjalankan aplikasi Anda. Untuk informasi selengkapnya, lihat [AWS layanan dalam produk ini](#).

Note

Anda bertanggung jawab atas biaya AWS layanan yang digunakan saat menjalankan produk ini.

Kami merekomendasikan membuat [anggaran](#) melalui [AWS Cost Explorer](#) untuk membantu mengelola biaya. Harga dapat berubah sewaktu-waktu. Untuk detail selengkapnya, lihat halaman web harga untuk setiap AWS layanan yang digunakan dalam produk ini.

Keamanan

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 model](#) menggambarkan ini sebagai keamanan 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 teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Studio Penelitian dan Rekayasa di AWS, lihat [AWS Layanan dalam Lingkup oleh AWS Layanan 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.

Untuk memahami bagaimana menerapkan model tanggung jawab bersama dengan AWS layanan yang digunakan oleh Research and Engineering Studio, lihat [Pertimbangan keamanan untuk layanan dalam produk ini](#). Untuk informasi lebih lanjut tentang AWS keamanan, kunjungi [AWS Cloud Keamanan](#).

Peran IAM

AWS Identity and Access Management (IAM) peran memungkinkan pelanggan untuk menetapkan kebijakan akses terperinci dan izin untuk layanan dan pengguna di. AWS Cloud Produk ini menciptakan peran IAM yang memberikan AWS Lambda fungsi produk dan EC2 instans Amazon akses untuk membuat sumber daya Regional.

RES mendukung kebijakan berbasis identitas dalam IAM. Saat digunakan, RES membuat kebijakan untuk menentukan izin dan akses administrator. Administrator yang mengimplementasikan produk membuat dan mengelola pengguna akhir dan pemimpin proyek dalam Active Directory pelanggan yang ada terintegrasi dengan RES. Untuk informasi selengkapnya, lihat [Membuat kebijakan IAM](#) di Panduan Pengguna AWS Identity and Access Management.

Administrator organisasi Anda dapat mengelola akses pengguna dengan direktori aktif. Saat pengguna akhir mengakses antarmuka pengguna RES, RES mengautentikasi dengan [Amazon Cognito](#).

Grup keamanan

Grup keamanan yang dibuat dalam produk ini dirancang untuk mengontrol dan mengisolasi lalu lintas jaringan antara fungsi Lambda EC2 , instance, instance CSR sistem file, dan titik akhir VPN jarak jauh. Kami menyarankan Anda meninjau grup keamanan dan membatasi akses lebih lanjut sesuai kebutuhan setelah produk digunakan.

Enkripsi data

Secara default, Research and Engineering Studio on AWS (RES) mengenkripsi data pelanggan saat istirahat dan dalam perjalanan menggunakan kunci yang dimiliki RES. Saat Anda menerapkan RES, Anda dapat menentukan file AWS KMS key. RES menggunakan kredensial Anda untuk memberikan

akses kunci. Jika Anda menyediakan pelanggan yang dimiliki dan dikelola AWS KMS key, data pelanggan saat istirahat akan dienkripsi menggunakan kunci itu.

RES mengenkripsi data pelanggan dalam perjalanan menggunakan SSL/TLS. Kami membutuhkan TLS 1.2, tetapi merekomendasikan TLS 1.3.

Pertimbangan keamanan untuk layanan dalam produk ini

Untuk informasi lebih rinci mengenai pertimbangan keamanan untuk layanan yang digunakan oleh Research and Engineering Studio, ikuti tautan dalam tabel ini:

AWS info keamanan layanan	Jenis layanan	Bagaimana layanan ini digunakan dalam RES
Amazon Elastic Compute Cloud	Core	Menyediakan layanan komputasi yang mendasari untuk membuat desktop virtual dengan sistem operasi dan tumpukan perangkat lunak pilihan mereka.
Elastic Load Balancing	Core	Host Bastion, cluster-mananager, dan VDI dibuat di grup Auto Scaling di belakang load balancer. ELB menyeimbangkan lalu lintas dari portal web di seluruh host RES.
Amazon Virtual Private Cloud	Core	Semua komponen produk inti dibuat dalam VPC Anda.
Amazon Cognito	Core	Mengelola identitas pengguna dan otentikasi. Pengguna Active Directory dipetakan ke pengguna dan grup Amazon Cognito untuk mengautentikasi tingkat akses.

AWS info keamanan layanan	Jenis layanan	Bagaimana layanan ini digunakan dalam RES
Sistem File Elastis Amazon	Core	Menyediakan sistem /home file untuk browser file dan host VDI, serta sistem file eksternal bersama.
Amazon DynamoDB	Core	Menyimpan data konfigurasi seperti pengguna, grup, proyek, sistem file, dan pengaturan komponen.
AWS Systems Manager	Core	Menyimpan dokumen untuk melakukan perintah untuk manajemen sesi VDI.
AWS Lambda	Core	Mendukung fungsionalitas produk seperti memperbaiki pengaturan dalam tabel DynamoDB, memulai alur kerja sinkronisasi Active Directory, dan memperbaiki daftar awalan.
Amazon CloudWatch	Mendukung	Menyediakan metrik dan log aktivitas untuk semua EC2 host Amazon dan fungsi Lambda.
Layanan Penyimpanan Sederhana Amazon	Mendukung	Menyimpan binari aplikasi untuk bootstrapping dan konfigurasi host.

AWS info keamanan layanan	Jenis layanan	Bagaimana layanan ini digunakan dalam RES
AWS Key Management Service	Mendukung	Digunakan untuk enkripsi saat istirahat dengan antrian Amazon SQS, tabel DynamoDB, dan topik Amazon SNS.
AWS Secrets Manager	Mendukung	Menyimpan kredensi akun layanan di Active Directory dan sertifikat yang ditandatangani sendiri untuk VDI
AWS CloudFormation	Mendukung	Menyediakan mekanisme penyebaran untuk produk.
AWS Identity and Access Management	Mendukung	Membatasi tingkat akses untuk host.
Route Amazon 53	Mendukung	Membuat zona host pribadi untuk menyelesaikan penyeimbang beban internal dan nama domain host bastion.
Amazon Simple Queue Service	Mendukung	Membuat antrian tugas untuk mendukung eksekusi asinkron.
Layanan Pemberitahuan Sederhana Amazon	Mendukung	Mendukung model publisasi-pelanggan antara komponen VDI seperti controller dan host.
AWS Fargate	Mendukung	Menginstal, memperbarui, dan menghapus lingkungan menggunakan tugas Fargate.

AWS info keamanan layanan	Jenis layanan	Bagaimana layanan ini digunakan dalam RES
Gerbang FSx File Amazon	Opsional	Menyediakan sistem file bersama eksternal.
Amazon FSx untuk NetApp ONTAP	Opsional	Menyediakan sistem file bersama eksternal.
AWS Certificate Manager	Opsional	Menghasilkan sertifikat terpercaya untuk domain kustom Anda.
AWS Backup	Opsional	Menawarkan kemampuan cadangan untuk EC2 host Amazon, sistem file, dan DynamoDB.

Kuota

Kuota layanan, juga disebut sebagai batas, adalah jumlah maksimum sumber daya layanan atau operasi untuk Anda Akun AWS.

Kuota untuk AWS layanan dalam produk ini

Pastikan Anda memiliki kuota yang cukup untuk setiap [layanan yang diterapkan dalam produk ini](#). Untuk informasi selengkapnya, lihat [AWS service quotas](#).

Untuk produk ini, kami sarankan menaikkan kuota untuk layanan berikut:

- Amazon Virtual Private Cloud
- Amazon EC2

Untuk meminta peningkatan kuota, lihat [Meminta Peningkatan Kuota](#) dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan [formulir penambahan batas](#).

AWS CloudFormation kuota

Anda Akun AWS memiliki AWS CloudFormation kuota yang harus Anda ketahui saat [meluncurkan tumpukan di](#) produk ini. Dengan memahami kuota ini, Anda dapat menghindari kesalahan pembatasan yang akan mencegah Anda menerapkan produk ini dengan sukses. Untuk informasi selengkapnya, lihat [AWS CloudFormation kuota](#) di Panduan AWS CloudFormation Pengguna.

Perencanaan ketahanan

Produk ini menyebarkan infrastruktur default dengan jumlah dan ukuran minimum EC2 instans Amazon untuk mengoperasikan sistem. Untuk meningkatkan ketahanan di lingkungan produksi skala besar, kami sarankan untuk meningkatkan pengaturan kapasitas minimum default dalam grup Auto Scaling (ASG) infrastruktur. Meningkatkan nilai dari satu instance menjadi dua instance memberikan manfaat dari beberapa Availability Zones (AZ) dan mengurangi waktu untuk memulihkan fungsionalitas sistem jika terjadi kehilangan data yang tidak terduga.

Pengaturan ASG dapat disesuaikan dalam EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>. Produk membuat empat secara ASGs default dengan setiap nama diakhiri dengan -asg. Anda dapat mengubah nilai minimum dan yang diinginkan ke jumlah yang sesuai untuk lingkungan produksi Anda. Pilih grup yang ingin Anda ubah, lalu pilih Tindakan dan pilih Edit. Untuk informasi selengkapnya ASGs, lihat [Menskalakan ukuran grup Auto Scaling Anda di Panduan](#) Pengguna Amazon Auto EC2 Scaling.

Didukung Wilayah AWS

Produk ini menggunakan layanan yang saat ini tidak tersedia di semua Wilayah AWS. Anda harus meluncurkan produk ini di Wilayah AWS mana semua layanan tersedia. Untuk ketersediaan AWS layanan terbaru menurut Wilayah, lihat [Daftar Layanan Wilayah AWS al](#).

Research and Engineering Studio on AWS didukung sebagai berikut Wilayah AWS:

Nama wilayah	Wilayah	Versi sebelumnya	Versi terbaru (2024.10)
US East (Northern Virginia)	us-east-1	Ya	Ya
US East (Ohio)	us-east-2	Ya	Ya

Nama wilayah	Wilayah	Versi sebelumnya	Versi terbaru (2024.10)
US West (N. California)	us-west-1	Ya	Ya
US West (Oregon)	us-west-2	Ya	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya	Ya
Canada (Central)	ca-central-1	Ya	Ya
Eropa (Frankfurt)	eu-central-1	Ya	Ya
Eropa (Milan)	eu-south-1	Ya	Ya
Eropa (Irlandia)	eu-west-1	Ya	Ya
Eropa (London)	eu-west-2	Ya	Ya
Europe (Paris)	eu-west-3	Ya	Ya
Eropa (Stockholm)	eu-north-1	tidak	Ya
Israel (Tel Aviv)	il-central-1	Ya	Ya
AWS GovCloud (AS-Barat)	us-gov-west-1	Ya	Ya

Menyebarkan produk

Note

Produk ini menggunakan [AWS CloudFormation templat dan tumpukan](#) untuk mengotomatiskan penerapannya. CloudFormationTemplate menjelaskan AWS sumber daya yang termasuk dalam produk ini dan propertinya. CloudFormation Tumpukan menyediakan sumber daya yang dijelaskan dalam template.

Sebelum Anda meluncurkan produk, tinjau [biaya](#), [arsitektur](#), [keamanan jaringan](#), dan pertimbangan lain yang dibahas sebelumnya dalam panduan ini.

Topik

- [Prasyarat](#)
- [Buat sumber daya eksternal](#)
- [Langkah 1: Luncurkan produk](#)
- [Langkah 2: Masuk untuk pertama kalinya](#)

Prasyarat

Topik

- [Buat Akun AWS dengan pengguna administratif](#)
- [Buat key pair Amazon EC2 SSH](#)
- [Tingkatkan kuota layanan](#)
- [Buat domain publik \(opsional\)](#)
- [Buat domain \(GovCloud hanya\)](#)
- [Menyediakan sumber daya eksternal](#)
- [Konfigurasi LDAPS di lingkungan Anda \(opsional\)](#)
- [Konfigurasi VPC pribadi \(opsional\)](#)

Buat Akun AWS dengan pengguna administratif

Anda harus memiliki Akun AWS dengan pengguna administratif:

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

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

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

Buat key pair Amazon EC2 SSH

Jika Anda tidak memiliki Amazon EC2 SSH key pair, Anda harus membuatnya. Untuk informasi selengkapnya, lihat [Membuat key pair menggunakan Amazon EC2](#) di Panduan EC2 Pengguna Amazon.

Tingkatkan kuota layanan

Kami merekomendasikan untuk [meningkatkan kuota layanan](#) untuk:

- [Amazon VPC](#)
 - Tingkatkan kuota alamat IP Elastic per gateway NAT dari lima menjadi delapan.
 - Tingkatkan gateway NAT per Availability Zone dari lima menjadi sepuluh.
- [Amazon EC2](#)
 - Tingkatkan EC2 -VPC Elastic IPs dari lima menjadi sepuluh

AWS Akun Anda memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan. Untuk informasi selengkapnya, lihat [Kuota untuk AWS layanan dalam produk ini](#).

Buat domain publik (opsional)

Sebaiknya gunakan domain khusus untuk produk agar memiliki URL yang ramah pengguna. Anda harus mendaftarkan domain menggunakan Amazon Route 53 atau penyedia lain dan mengimpor sertifikat untuk domain yang digunakan AWS Certificate Manager. Jika Anda sudah memiliki domain publik dan sertifikat, Anda dapat melewati langkah ini.

1. Ikuti petunjuk untuk [mendaftarkan domain dengan](#) Route53. Anda harus menerima email konfirmasi.
2. Ambil zona yang dihosting untuk domain Anda. Ini dibuat secara otomatis oleh Route53.
 - a. Buka konsol Route53.
 - b. Pilih Zona yang dihosting dari navigasi kiri.
 - c. Buka zona host yang dibuat untuk nama domain Anda dan salin ID zona Hosted.
3. Buka AWS Certificate Manager dan ikuti langkah-langkah berikut untuk [meminta sertifikat domain](#). Pastikan Anda berada di Wilayah tempat Anda berencana untuk menerapkan solusi.
4. Pilih Daftar sertifikat dari navigasi, dan temukan permintaan sertifikat Anda. Permintaan harus tertunda.
5. Pilih ID Sertifikat Anda untuk membuka permintaan.
6. Dari bagian Domain, pilih Buat catatan di Route53. Diperlukan waktu sekitar sepuluh menit untuk memproses permintaan.
7. Setelah sertifikat dikeluarkan, salin ARN dari bagian status Sertifikat.

Buat domain (GovCloud hanya)

Jika Anda menerapkan di Wilayah AWS GovCloud (AS-Barat) dan Anda menggunakan domain khusus untuk Studio Penelitian dan Teknik, Anda harus menyelesaikan langkah-langkah prasyarat ini.

1. Menerapkan [AWS CloudFormation tumpukan Sertifikat](#) di AWS Akun partisi komersial tempat domain yang dihosting publik dibuat.
2. Dari CloudFormation Output Sertifikat, temukan dan catat `CertificateARN` dan `PrivateKeySecretARN`.

3. Di akun GovCloud partisi, buat rahasia dengan nilai `CertificateArn` output. Perhatikan ARN rahasia baru dan tambahkan dua tag ke rahasia sehingga `vdc-gateway` dapat mengakses nilai rahasia:
 - a. `res: ModuleName = virtual-desktop-controller`
 - b. `res: EnvironmentName = [nama lingkungan]` (Ini bisa berupa `res-demo`.)
4. Di akun GovCloud partisi, buat rahasia dengan nilai `PrivateKeySecretArn` output. Perhatikan ARN rahasia baru dan tambahkan dua tag ke rahasia sehingga `vdc-gateway` dapat mengakses nilai rahasia:
 - a. `res: ModuleName = virtual-desktop-controller`
 - b. `res: EnvironmentName = [nama lingkungan]` (Ini bisa berupa `res-demo`.)

Menyediakan sumber daya eksternal

Research and Engineering Studio on AWS mengharapkan sumber daya eksternal berikut ada saat digunakan.

- Jaringan (VPC, Subnet Publik, dan Subnet Pribadi)

Di sinilah Anda akan menjalankan EC2 instance yang digunakan untuk meng-host lingkungan RES, Active Directory (AD), dan penyimpanan bersama.

- Penyimpanan (Amazon EFS)

Volume penyimpanan berisi file dan data yang diperlukan untuk infrastruktur desktop virtual (VDI).

- Layanan direktori (AWS Directory Service for Microsoft Active Directory)

Layanan direktori mengautentikasi pengguna ke lingkungan RES.

- Rahasia yang berisi nama pengguna dan kata sandi akun layanan Active Directory yang diformat sebagai pasangan nilai kunci (nama pengguna, kata sandi)

Studio Riset dan Teknik mengakses [rahasia](#) yang Anda berikan, termasuk kata sandi akun layanan, menggunakan [AWS Secrets Manager](#).

 Tip

Jika Anda menerapkan lingkungan demo dan tidak memiliki sumber daya eksternal ini, Anda dapat menggunakan resep Komputasi Kinerja AWS Tinggi untuk menghasilkan sumber daya eksternal. Lihat bagian berikut, [Buat sumber daya eksternal](#), untuk menyebarkan sumber daya di akun Anda.

Untuk penerapan demo di Wilayah AWS GovCloud (AS-Barat), Anda harus menyelesaikan langkah-langkah prasyarat di [Buat domain \(GovCloud hanya\)](#)

Konfigurasikan LDAPS di lingkungan Anda (opsional)

Jika Anda berencana untuk menggunakan komunikasi LDAPS di lingkungan Anda, Anda harus menyelesaikan langkah-langkah ini untuk membuat dan melampirkan sertifikat ke pengontrol domain AWS Managed Microsoft AD (AD) untuk menyediakan komunikasi antara AD dan RES.

1. Ikuti langkah-langkah yang disediakan di [Cara mengaktifkan LDAPS sisi server](#) untuk Anda. AWS Managed Microsoft AD Anda dapat melewati langkah ini jika Anda telah mengaktifkan LDAPS.
2. Setelah mengonfirmasi bahwa LDAPS dikonfigurasi pada AD, ekspor sertifikat AD:
 - a. Buka server Active Directory Anda.
 - b. Buka PowerShell sebagai administrator.
 - c. Jalankan `certmgr.msc` untuk membuka daftar sertifikat.
 - d. Buka daftar sertifikat dengan terlebih dahulu membuka Otoritas Sertifikasi Root Tepercaya dan kemudian Sertifikat.
 - e. Pilih dan tahan (atau klik kanan) sertifikat dengan nama yang sama dengan server AD Anda dan pilih Semua tugas lalu Ekspor.
 - f. Pilih Base-64 yang dikodekan X.509 (.CER) dan pilih Berikutnya.
 - g. Pilih direktori dan kemudian pilih Berikutnya.
3. Buat rahasia di AWS Secrets Manager:

Saat membuat Secret Anda di Secrets Manager, pilih Jenis rahasia lain di bawah tipe rahasia dan tempel sertifikat yang dikodekan PEM Anda di bidang Plaintext.

4. Perhatikan ARN yang dibuat dan masukkan sebagai `DomainTLSCertificateSecretARN` parameter di [Langkah 1: Luncurkan produk](#)

Konfigurasi VPC pribadi (opsional)

Menyebarkan Studio Penelitian dan Teknik di VPC yang terisolasi menawarkan keamanan yang ditingkatkan untuk memenuhi persyaratan kepatuhan dan tata kelola organisasi Anda. Namun, penerapan RES standar bergantung pada akses internet untuk menginstal dependensi. Untuk menginstal RES di VPC pribadi, Anda harus memenuhi prasyarat berikut:

Topik

- [Siapkan Gambar Mesin Amazon \(AMIs\)](#)
- [Siapkan titik akhir VPC](#)
- [Connect ke layanan tanpa titik akhir VPC](#)
- [Tetapkan parameter penyebaran VPC pribadi](#)

Siapkan Gambar Mesin Amazon (AMIs)

1. Unduh [dependensi](#). Untuk menyebarkan di VPC terisolasi, infrastruktur RES membutuhkan ketersediaan dependensi tanpa memiliki akses internet publik.
2. Buat peran IAM dengan akses hanya-baca Amazon S3 dan identitas tepercaya sebagai Amazon. EC2
 - a. Buka konsol IAM di <https://console.aws.amazon.com/iam/>.
 - b. Dari Peran, pilih Buat peran.
 - c. Pada halaman Pilih entitas tepercaya:
 - Di bawah Jenis entitas tepercaya, pilih Layanan AWS.
 - Untuk kasus penggunaan di bawah Layanan atau kasus penggunaan, pilih EC2 dan pilih Berikutnya.
 - d. Pada Tambahkan izin, pilih kebijakan izin berikut, lalu pilih Berikutnya:
 - AmazonS3 ReadOnlyAccess
 - AmazonSSMManagedInstanceCore
 - EC2InstanceProfileForImageBuilder
 - e. Tambahkan nama Peran dan Deskripsi, lalu pilih Buat peran.
3. Buat komponen pembuat EC2 gambar:
 - a. Buka konsol EC2 Image Builder di <https://console.aws.amazon.com/imagebuilder>.

- b. Di bawah Sumber daya tersimpan, pilih Komponen dan pilih Buat komponen.
- c. Pada halaman Create component, masukkan detail berikut:
 - Untuk tipe Component, pilih Build.
 - Untuk detail Komponen pilih:

Parameter	Entri pengguna
Sistem operasi gambar (OS)	Linux
Versi OS yang Kompatibel	Amazon Linux 2, RHEL8, atau RHEL9
Nama komponen	Masukkan nama seperti: <i><research-and-engineering-studio-infrastructure></i>
Versi komponen	Kami merekomendasikan memulai dengan 1.0.0.
Deskripsi	Entri pengguna opsional.

- d. Pada halaman Buat komponen, pilih Tentukan konten dokumen.
 - i. Sebelum memasukkan konten dokumen definisi, Anda akan memerlukan URI file untuk file tar.gz. Unggah file tar.gz yang disediakan oleh RES ke bucket Amazon S3 dan salin URI file dari properti bucket.
 - ii. Masukkan yang berikut ini:

 Note

AddEnvironmentVariables bersifat opsional, dan Anda dapat menghapusnya jika Anda tidak memerlukan variabel lingkungan khusus di host infrastruktur Anda.

Jika Anda menyiapkan http_proxy dan variabel https_proxy lingkungan, no_proxy parameter diperlukan untuk mencegah instance menggunakan proxy untuk menanyakan localhost, alamat IP metadata instance, dan layanan yang mendukung titik akhir VPC.

```

# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the "License"). You may
# not use this file except in compliance
# with the License. A copy of the License is located at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# or in the 'license' file accompanying this file. This file is
# distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
# OR CONDITIONS OF ANY KIND, express or implied. See the License for the
# specific language governing permissions
# and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
  software dependencies for infrastructure hosts.
schemaVersion: 1.0

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
      - name: DownloadRESInstallScripts
        action: S3Download
        onFailure: Abort
        maxAttempts: 3
        inputs:
          - source: '<s3 tar.gz file uri>'
            destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
            expectedBucketOwner: '{{ AWSAccountID }}'
      - name: RunInstallScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:

```

```

        commands:
          - 'cd /root/bootstrap/res_dependencies'
          - 'tar -xf res_dependencies.tar.gz'
          - 'cd all_dependencies'
          - '/bin/bash install.sh'
- name: AddEnvironmentVariables
  action: ExecuteBash
  onFailure: Abort
  maxAttempts: 3
  inputs:
    commands:
      - |
        echo -e "
        http_proxy=http://<ip>:<port>
        https_proxy=http://<ip>:<port>

        no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
        {{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
        {{ AWSRegion }}.elb.amazonaws.com,s3.
        {{ AWSRegion }}.amazonaws.com,s3.dualstack.
        {{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
        {{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
        {{ AWSRegion }}.amazonaws.com,ssmmessages.
        {{ AWSRegion }}.amazonaws.com,kms.
        {{ AWSRegion }}.amazonaws.com,secretsmanager.
        {{ AWSRegion }}.amazonaws.com,sqs.
        {{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
        {{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
        {{ AWSRegion }}.amazonaws.com,logs.
        {{ AWSRegion }}.api.aws,elasticfilesystem.
        {{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
        {{ AWSRegion }}.amazonaws.com,api.ecr.
        {{ AWSRegion }}.amazonaws.com,.dkr.ecr.
        {{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
        kinesis.{{ AWSRegion }}.amazonaws.com,.control-
        kinesis.{{ AWSRegion }}.amazonaws.com,events.
        {{ AWSRegion }}.amazonaws.com,cloudformation.
        {{ AWSRegion }}.amazonaws.com,sts.
        {{ AWSRegion }}.amazonaws.com,application-autoscaling.
        {{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com,ecs.
        {{ AWSRegion }}.amazonaws.com,.execute-api.{{ AWSRegion }}.amazonaws.com
        >
        " > /etc/environment

```

e. Pilih Buat komponen.

4. Buat resep gambar Image Builder.

- a. Pada halaman Buat resep, masukkan yang berikut ini:

Bagian	Parameter	Entri pengguna
Detail resep	Nama	Masukkan nama yang sesuai seperti res-recipe-linux-x 86.
	Versi	Masukkan versi, biasanya dimulai dengan 1.0.0.
	Deskripsi	Tambahkan deskripsi opsional.
Gambar dasar	Pilih gambar	Pilih gambar terkelola.
	OS	Amazon Linux atau Red Hat Enterprise Linux (RHEL)
	Asal gambar	Mulai cepat (dikelola Amazon)
	Nama gambar	Amazon Linux 2 x86, Red Hat Enterprise Linux 8 x86, atau Red Hat Enterprise Linux 9 x86
	Opsi versi otomatis	Gunakan versi OS terbaru yang tersedia.
Konfigurasi instans	–	Simpan semuanya dalam pengaturan default, dan pastikan Hapus agen SSM setelah eksekusi pipeline tidak dipilih.

Bagian	Parameter	Entri pengguna
Direktori kerja	Jalur direktori kerja	/root/bootstrap/res_dependencies
Komponen	Membangun komponen	Cari dan pilih yang berikut ini: • Dikelola Amazon: -2-linux aws-cli-version • Dikelola Amazon: amazon-cloudwatch-agent-linux • Dimiliki oleh Anda: EC2 Komponen Amazon yang dibuat sebelumnya a. Masukkan Akun AWS ID Anda dan saat ini Wilayah AWS di bidang.
	Komponen uji	Cari dan pilih: • Dikelola Amazon: simple-boot-test-linux

b. Pilih Buat resep.

5. Buat konfigurasi infrastruktur Image Builder.

- Di bawah Sumber daya tersimpan, pilih Konfigurasi infrastruktur.
- Pilih Buat konfigurasi infrastruktur.
- Pada halaman Buat konfigurasi infrastruktur, masukkan yang berikut ini:

Bagian	Parameter	Entri pengguna
Umum	Nama	Masukkan nama yang sesuai seperti res-infra-linux-x 86.

Bagian	Parameter	Entri pengguna
	Deskripsi	Tambahkan deskripsi opsional.
	Peran IAM	Pilih peran IAM yang dibuat sebelumnya.
AWS Infrastruktur	Jenis instans	Pilih t3.medium.
	VPC, subnet, dan grup keamanan	Pilih opsi yang memungkinkan akses internet dan akses ke bucket Amazon S3. Jika Anda perlu membuat grup keamanan, Anda dapat membuatnya dari EC2 konsol Amazon dengan input berikut: • VPC: Pilih VPC yang sama yang digunakan untuk konfigurasi infrastruktur. VPC ini harus memiliki akses internet. • Aturan masuk: • Jenis: SSH • Sumber: Kustom • Blok CIDR: 0.0.0.0/0

d. Pilih Buat konfigurasi infrastruktur.

6. Buat pipeline EC2 Image Builder baru:

a. Buka pipeline Image, dan pilih Create image pipeline.

b. Pada halaman Tentukan rincian pipeline, masukkan yang berikut ini dan pilih Berikutnya:

- Nama pipa dan deskripsi opsional

- Untuk jadwal Build, atur jadwal atau pilih Manual jika Anda ingin memulai proses baking AMI secara manual.
 - c. Pada halaman Pilih resep, pilih Gunakan resep yang ada dan masukkan nama Resep yang dibuat sebelumnya. Pilih Berikutnya.
 - d. Pada halaman Tentukan proses gambar, pilih alur kerja default dan pilih Berikutnya.
 - e. Pada halaman Tentukan konfigurasi infrastruktur, pilih Gunakan konfigurasi infrastruktur yang ada dan masukkan nama konfigurasi infrastruktur yang dibuat sebelumnya. Pilih Berikutnya.
 - f. Pada halaman Tentukan pengaturan distribusi, pertimbangkan hal berikut untuk pilihan Anda:
 - Gambar keluaran harus berada di wilayah yang sama dengan lingkungan RES yang diterapkan, sehingga RES dapat meluncurkan instance host infrastruktur dengan benar darinya. Menggunakan default layanan, gambar output akan dibuat di wilayah tempat layanan EC2 Image Builder digunakan.
 - Jika Anda ingin menerapkan RES di beberapa wilayah, Anda dapat memilih Buat pengaturan distribusi baru dan menambahkan lebih banyak wilayah di sana.
 - g. Tinjau pilihan Anda dan pilih Buat pipeline.
7. Jalankan pipeline EC2 Image Builder:
- a. Dari pipeline Image, temukan dan pilih pipeline yang Anda buat.
 - b. Pilih Tindakan, lalu pilih Jalankan pipeline.
- Pipa mungkin memakan waktu sekitar 45 menit hingga satu jam untuk membuat gambar AMI.
8. Perhatikan ID AMI untuk AMI yang dihasilkan dan gunakan sebagai input untuk parameter InfrastructureHost AMI di [the section called “Langkah 1: Luncurkan produk”](#).

Siapkan titik akhir VPC

Untuk menyebarkan RES dan meluncurkan desktop virtual, Layanan AWS memerlukan akses ke subnet pribadi Anda. Anda harus menyiapkan titik akhir VPC untuk menyediakan akses yang diperlukan, dan Anda harus mengulangi langkah-langkah ini untuk setiap titik akhir.

1. Jika titik akhir belum dikonfigurasi sebelumnya, ikuti petunjuk yang disediakan di [Akses Layanan AWS menggunakan titik akhir VPC antarmuka](#).

2. Pilih satu subnet pribadi di masing-masing dari dua zona ketersediaan.

Layanan AWS	Nama layanan
Application Auto Scaling	com.amazonaws. <i>region</i> .application-autoscaling
AWS CloudFormation	com.amazonaws. <i>region</i> .cloudformasi
Amazon CloudWatch	com.amazonaws. <i>region</i> .pemantauan
CloudWatch Log Amazon	com.amazonaws. <i>region</i> .log
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb (Membutuhkan titik akhir gateway)
Amazon EC2	com.amazonaws. <i>region</i> .ec2
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
Sistem File Elastis Amazon	com.amazonaws. <i>region</i> .elasticfilesystem
Elastic Load Balancing	com.amazonaws. <i>region</i> .elasticloadbalancing
Amazon EventBridge	com.amazonaws. <i>region</i> .acara
Amazon FSx	com.amazonaws. <i>region</i> .fsx
AWS Key Management Service	com.amazonaws. <i>region</i> .kms
Amazon Kinesis Data Streams	com.amazonaws. <i>region</i> .kinesis-stream
AWS Lambda	com.amazonaws. <i>region</i> .lambda
Amazon S3	com.amazonaws. <i>region</i> .s3 (Membutuhkan titik akhir gateway yang dibuat secara default di RES.) Titik akhir antarmuka Amazon S3 tambahan diperlukan untuk bucket pemasangan silang di lingkungan yang

Layanan AWS	Nama layanan
	terisolasi. Lihat Mengakses titik akhir antarmuka Layanan Penyimpanan Sederhana Amazon .
AWS Secrets Manager	com.amazonaws. <i>region</i> .secretsmanager
Layanan Kontainer Elastis Amazon	com.amazonaws. <i>region</i> .ecs
Amazon SES	com.amazonaws. <i>region</i> .email-smtp (Tidak didukung di Availability Zone berikut: use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3, dan cac1-az4.)
AWS Security Token Service	com.amazonaws. <i>region</i> .sts
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> .sqs
AWS Systems Manager	com.amazonaws. <i>region</i> .ec2pesan
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> .ssmmessages

Connect ke layanan tanpa titik akhir VPC

Untuk mengintegrasikan dengan layanan yang tidak mendukung titik akhir VPC, Anda dapat mengatur server proxy di subnet publik VPC Anda. Ikuti langkah-langkah ini untuk membuat server proxy dengan akses minimum yang diperlukan untuk penyebaran Studio Riset dan Teknik menggunakan AWS Identity Center sebagai penyedia identitas Anda.

1. Luncurkan instance Linux di subnet publik VPC yang akan Anda gunakan untuk penyebaran RES Anda.
 - Keluarga Linux - Amazon Linux 2 atau Amazon Linux 3
 - Arsitektur — x86
 - Jenis instans - t2.micro atau lebih tinggi

- Grup keamanan — TCP pada port 3128 dari 0.0.0.0/0
2. Connect ke instance untuk menyiapkan server proxy.
 - a. Buka koneksi http.
 - b. Izinkan koneksi ke domain berikut dari semua subnet yang relevan:
 - .amazonaws.com (untuk layanan generik) AWS
 - .amazoncognito.com (untuk Amazon Cognito)
 - .awsapps.com (untuk Pusat Identitas)
 - .signin.aws (untuk Pusat Identitas)
 - .amazonaws-us-gov.com (untuk Gov Cloud)
 - c. Tolak semua koneksi lainnya.
 - d. Aktifkan dan mulai server proxy.
 - e. Perhatikan PORT tempat server proxy mendengarkan.
 3. Konfigurasi tabel rute Anda untuk memungkinkan akses ke server proxy.
 - a. Buka konsol VPC Anda dan identifikasi tabel rute untuk subnet yang akan Anda gunakan untuk Host Infrastruktur dan host VDI.
 - b. Edit tabel rute untuk memungkinkan semua koneksi masuk ke instance server proxy yang dibuat pada langkah sebelumnya.
 - c. Lakukan ini untuk tabel rute untuk semua subnet (tanpa akses internet) yang akan Anda gunakan untuk InfrastrukturVDIs/.
 4. Ubah grup keamanan EC2 instance server proxy dan pastikan itu memungkinkan koneksi TCP masuk pada PORT tempat server proxy mendengarkan.

Tetapkan parameter penyebaran VPC pribadi

Dit [the section called “Langkah 1: Luncurkan produk”](#), Anda diharapkan untuk memasukkan parameter tertentu dalam AWS CloudFormation template. Pastikan untuk mengatur parameter berikut seperti yang dicatat agar berhasil disebarkan ke VPC pribadi yang baru saja Anda konfigurasi.

Parameter	Input
InfrastructureHostAMI	Gunakan ID AMI infrastruktur yang dibuat di the section called “Siapkan Gambar Mesin Amazon (AMIs)” .
IsLoadBalancerInternetFacing	Setel ke false.
LoadBalancerSubnets	Pilih subnet pribadi tanpa akses internet.
InfrastructureHostSubnets	Pilih subnet pribadi tanpa akses internet.
VdiSubnets	Pilih subnet pribadi tanpa akses internet.
ClientIP	Anda dapat memilih CIDR VPC Anda untuk memungkinkan akses ke semua alamat IP VPC.
HttpProxy	Contoh: <code>http://10.1.2.3:123</code>
HttpsProxy	Contoh: <code>http://10.1.2.3:123</code>
NoProxy	Contoh: <pre>127.0.0.1,169.254.169.254,169.254.170.2,localhost,us-east-1.res,us-east-1.vpce.amazonaws.com,us-east-1.elb.amazonaws.com,s3.us-east-1.amazonaws.com,s3.dualstack.us-east-1.amazonaws.com,ec2.us-east-1.amazonaws.com,ec2.us-east-1.api.aws,ec2messages.us-east-1.amazonaws.com,ssm.us-east-1.amazonaws.com,ssmmessages.us-east-1.amazonaws.com,kms.us-east-1.amazonaws.com,secretsmanager.us-east-1.amazonaws.com,sqs.us-east-1.amazonaws.com,elasticloadbalancing.us-east-1.amazonaws.com,sns.us-east-1.amazonaws.com,logs.us-east-1.amazonaws.com,logs.us-east-1.api.aws,elasticfilesystem.us-east-1.amazonaws.com,fsx.us-east-1.amazonaws.com,dynamodb.us-east-1.amaz</pre>

Parameter

Input

```
onaws.com,api.ecr.us-east-1.amazonaws.com,.dkr.ecr.us-east-1.amazonaws.com,kinesis.us-east-1.amazonaws.com,.data-kinesis.us-east-1.amazonaws.com,.control-kinesis.us-east-1.amazonaws.com,events.us-east-1.amazonaws.com,cloudformation.us-east-1.amazonaws.com,sts.us-east-1.amazonaws.com,application-autoscaling.us-east-1.amazonaws.com,monitoring.us-east-1.amazonaws.com,ecs.us-east-1.amazonaws.com,.execute-api.us-east-1.amazonaws.com
```

Buat sumber daya eksternal

CloudFormation Tumpukan ini menciptakan jaringan, penyimpanan, direktori aktif, dan sertifikat domain (jika PortalDomainName disediakan). Anda harus memiliki sumber daya eksternal ini tersedia untuk menyebarkan produk.

Anda dapat [mengunduh template resep](#) sebelum penerapan.

Waktu untuk menyebarkan: Sekitar 40-90 menit

1. Masuk ke AWS Management Console dan buka AWS CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.

Note

Pastikan Anda berada di akun administrator Anda.

2. [Luncurkan template](#) di konsol.

Jika Anda menerapkan di Wilayah AWS GovCloud (AS-Barat), [luncurkan template di akun GovCloud partisi](#).

3. Masukkan parameter template:

Parameter	Default	Deskripsi
DomainName	corp.res.com	Domain digunakan untuk direktori aktif. Nilai default disediakan dalam LDIF file yang mengatur pengguna bootstrap. Jika Anda ingin menggunakan pengguna default, biarkan nilainya sebagai default. Untuk mengubah nilai, perbarui dan berikan LDIF file terpisah. Ini tidak perlu cocok dengan domain yang digunakan untuk direktori aktif.
SubDomain (GovCloud hanya)		Parameter ini opsional untuk wilayah komersial, tetapi diperlukan untuk GovCloud wilayah. Jika Anda memberikan SubDomain, parameter akan diawali dengan yang DomainName disediakan. Nama domain Active Directory yang disediakan akan menjadi subdomain.

Parameter	Default	Deskripsi
AdminPassword		Kata sandi untuk administrator direktori aktif (nama penggunaAdmin). Pengguna ini dibuat di direktori aktif untuk fase bootstrap awal dan tidak digunakan setelahnya. Penting: format bidang ini dapat berupa (1) kata sandi teks biasa atau (2) ARN AWS Rahasia yang diformat sebagai pasangan. key/value {"password": "somepassword"} Catatan: Kata sandi untuk pengguna ini harus memenuhi persyaratan kompleksitas kata sandi untuk direktori aktif.

Parameter	Default	Deskripsi
ServiceAccountPassword		Kata sandi yang digunakan untuk membuat akun layanan (ReadOnlyUser). Akun ini digunakan untuk sinkronisasi. Penting: format bidang ini dapat berupa (1) kata sandi teks biasa atau (2) ARN AWS Rahasia yang diformat sebagai pasangan. key/value {"password": "somepassword"} Catatan: Kata sandi untuk pengguna ini harus memenuhi persyaratan kompleksitas kata sandi untuk direktori aktif.
Keypair		Menghubungkan instans administratif menggunakan klien SSH. Catatan: AWS Systems Manager Session Manager juga dapat digunakan untuk menyambung ke instance.

Parameter	Default	Deskripsi
LDIFS3Jalan	aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif	Jalur Amazon S3 ke file LDIF yang diimpor selama fase bootstrap pengaturan direktori aktif. Untuk informasi selengkapnya, lihat Dukungan LDIF. Parameter diisi sebelumnya dengan file yang membuat sejumlah pengguna di direktori aktif. Untuk melihat file, lihat file res.ldif yang tersedia di file. GitHub
ClientIpCidr		Alamat IP dari mana Anda akan mengakses situs. Misalnya, Anda dapat memilih alamat IP Anda dan menggunakannya [IPADDRESS]/32 untuk hanya mengizinkan akses dari host Anda. Anda dapat memperbarui pasca-penerapan ini.
ClientPrefixList		Masukkan daftar awalan untuk menyediakan akses ke node manajemen direktori aktif. Untuk informasi tentang cara membuat daftar awalan terkelola, lihat Bekerja dengan daftar awalan yang dikelola pelanggan.

Parameter	Default	Deskripsi
EnvironmentName	res- <i>[environment name]</i>	Jika PortalDomainName disediakan, parameter ini digunakan untuk menambahkan tag ke rahasia yang dihasilkan sehingga mereka dapat digunakan dalam lingkungan. Ini harus cocok dengan EnvironmentName parameter yang digunakan saat membuat tumpukan RES. Jika Anda menerapkan beberapa lingkungan di akun Anda, ini harus unik.
PortalDomainName		Untuk GovCloud penerapan, jangan masukkan parameter ini. Sertifikat dan rahasia dibuat secara manual selama prasyarat. Nama domain di Amazon Route 53 untuk akun tersebut. Jika ini disediakan, maka sertifikat publik dan file kunci akan dibuat dan diunggah ke AWS Secrets Manager. Jika Anda memiliki domain dan sertifikat Anda sendiri, parameter ini dan EnvironmentName dapat dibiarkan kosong.

4. Akui semua kotak centang di Capabilities, dan pilih Create stack.

Langkah 1: Luncurkan produk

Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menyebarkan produk ke akun Anda.

Waktu untuk menyebarkan: Sekitar 60 menit

Anda dapat [mengunduh CloudFormation template](#) untuk produk ini sebelum menerapkannya.

[Jika Anda menerapkan di AWS GovCloud \(AS-Barat\), gunakan template ini.](#)

res-stack - Gunakan template ini untuk meluncurkan produk dan semua komponen terkait. Konfigurasi default menyebarkan sumber daya tumpukan dan autentikasi utama RES, frontend, dan backend.

Note

AWS CloudFormation sumber daya dibuat dari AWS Cloud Development Kit (AWS CDK) (AWS CDK) konstruksi.

AWS CloudFormation Template menyebarkan Research and Engineering Studio AWS di. AWS Cloud Anda harus memenuhi [prasyarat](#) sebelum meluncurkan tumpukan.

1. Masuk ke AWS Management Console dan buka AWS CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Luncurkan [template](#).

[Untuk menyebarkan di AWS GovCloud \(AS-Barat\), luncurkan template ini.](#)

3. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di tempat lain Wilayah AWS, gunakan pemilih Wilayah di bilah navigasi konsol.

Note

Produk ini menggunakan layanan Amazon Cognito, yang saat ini tidak tersedia di semua. Wilayah AWS Anda harus meluncurkan produk ini di Wilayah AWS tempat Amazon Cognito tersedia. Untuk ketersediaan terbaru menurut Wilayah, lihat [Daftar Layanan Wilayah AWS](#) al.

4. Di bawah Parameter, tinjau parameter untuk templat produk ini dan modifikasi sesuai kebutuhan. Jika Anda menggunakan sumber daya eksternal otomatis, Anda dapat menemukan parameter ini di tab Output dari tumpukan sumber daya eksternal.

Parameter	Default	Deskripsi
EnvironmentName	<i><res-demo></i>	Nama unik yang diberikan ke lingkungan RES Anda dimulai dengan res-, tidak lebih dari 11 karakter, dan tidak ada huruf kapital.
AdministratorEmail		Alamat email untuk pengguna yang menyelesaikan penyiapan produk. Pengguna ini juga berfungsi sebagai pengguna break-glass jika ada tanda tunggal direktori aktif pada kegagalan integrasi.
InfrastructureHostAMI	ami- <i>[numbers or letters only]</i>	(Opsional) Anda dapat memberikan id AMI khusus untuk digunakan untuk semua host infrastruktur. Yang didukung saat ini OSES adalah Amazon Linux 2, RHEL8, atau RHEL9. Untuk informasi selengkapnya, lihat Siapkan Gambar Mesin Amazon (AMIs) .
SSHKeyPasangan		Key pair digunakan untuk terhubung ke host infrastruktur.

Parameter	Default	Deskripsi
ClientIP	<code>x.x.x.0/24</code> atau <code>.0/32</code> <code>x.x.x</code>	Filter alamat IP yang membatasi koneksi ke sistem. Anda dapat memperbarui ClientIpCidr setelah penerapan.
ClientPrefixList		(Opsional) Berikan daftar awalan terkelola agar IPs diizinkan mengakses UI web dan SSH secara langsung ke host bastion.
IAMPermissionBatas		(Opsional) Anda dapat memberikan ARN kebijakan terkelola yang akan dilampirkan sebagai batas izin untuk semua peran yang dibuat di RES. Untuk informasi selengkapnya, lihat Menetapkan batas izin khusus .
VpcId		ID untuk VPC tempat instance akan diluncurkan.
IsLoadBalancerInternetFacing		Pilih true untuk menyebarkan penyeimbang beban yang menghadap internet (Memerlukan subnet publik untuk penyeimbang beban). Untuk penerapan yang memerlukan akses internet terbatas, pilih false.

Parameter	Default	Deskripsi
LoadBalancerSubnets		Pilih setidaknya dua subnet di Availability Zone yang berbeda di mana load balancer akan diluncurkan. Untuk penerapan yang memerlukan akses internet terbatas, pilih subnet pribadi. Untuk penerapan yang membutuhkan akses internet, pilih subnet publik. Jika lebih dari dua dibuat oleh tumpukan jaringan eksternal, pilih semua yang dibuat.
InfrastructureHostSubnets		Pilih setidaknya dua subnet pribadi di Availability Zone yang berbeda di mana host infrastruktur akan diluncurkan. Jika lebih dari dua dibuat oleh tumpukan jaringan eksternal, pilih semua yang dibuat.
VdiSubnets		Pilih setidaknya dua subnet pribadi di Availability Zone yang berbeda di mana instans VDI akan diluncurkan. Jika lebih dari dua dibuat oleh tumpukan jaringan eksternal, pilih semua yang dibuat.

Parameter	Default	Deskripsi
ActiveDirectoryName	<i>corp.res.com</i>	Domain untuk direktori aktif. Tidak perlu mencocokkan nama domain portal.
ADShortNama	<i>corp</i>	Nama singkat untuk direktori aktif. Ini juga disebut nama NetBIOS.
Basis LDAP	<i>DC=corp,DC=res,DC=com</i>	Jalur LDAP ke basis dalam hierarki LDAP.
LDAPConnectionURI		Jalur ldap://tunggal yang dapat dicapai oleh server host direktori aktif. Jika Anda menerapkan sumber daya eksternal otomatis dengan domain AD default, Anda dapat menggunakan ldap: // corp.res.com.
ServiceAccountCredentialsSecretArn		Berikan ARN Rahasia yang berisi nama pengguna dan kata sandi untuk pengguna Active Directory, diformat sebagai pasangan nama ServiceAccount pengguna: kata sandi. key/value
UserSou		Unit organisasi dalam AD untuk pengguna yang akan melakukan sinkronisasi.
GroupSou		Unit organisasi dalam AD untuk grup yang akan disinkronkan.

Parameter	Default	Deskripsi
SudoersGroupName	RESAdministrators	Nama grup yang berisi semua pengguna dengan akses sudoer pada instance saat menginstal dan akses administrator di RES.
KomputerSOU		Unit organisasi dalam AD yang instans akan bergabung.
TLSCertificateSecretARN Domain		(Opsional) Menyediakan ARN rahasia sertifikat TLS domain untuk mengaktifkan komunikasi TLS ke AD.
EnableLdapIDMapping		Menentukan apakah nomor UID dan GID dihasilkan oleh SSSD atau jika nomor yang disediakan oleh AD digunakan. Setel ke True untuk menggunakan UID dan GID yang dihasilkan SSSD, atau False untuk menggunakan UID dan GID yang disediakan oleh AD. Untuk kebanyakan kasus parameter ini harus diatur ke True.
Nonaktifkan ADJoin	False	Untuk mencegah host Linux bergabung dengan domain direktori, ubah ke True. Jika tidak, biarkan dalam pengaturan default False.

Parameter	Default	Deskripsi
ServiceAccountUserDN		Berikan nama terhormat (DN) dari pengguna akun layanan di Direktori.
SharedHomeFilesystemID		ID EFS yang digunakan untuk sistem file rumah bersama untuk host VDI Linux.
CustomDomainNameforWebApp		(Opsional) Subdomain yang digunakan oleh portal web untuk menyediakan tautan untuk bagian web sistem.
CustomDomainNameforVDI		(Opsional) Subdomain yang digunakan oleh portal web untuk menyediakan tautan untuk bagian VDI dari sistem.

Parameter	Default	Deskripsi
ACMCertificateARNforWebApp		(Opsional) Saat menggunakan konfigurasi default, produk meng-host aplikasi web di bawah domain amazonaws.com. Anda dapat meng-host layanan produk di bawah domain Anda. Jika Anda menerapkan sumber daya eksternal otomatis, ini dibuat untuk Anda dan informasinya dapat ditemukan di Output dari tumpukan res-bi. Jika Anda perlu membuat sertifikat untuk aplikasi web Anda, lihat Panduan konfigurasi .
CertificateSecretARNforVDI		(Opsional) Rahasia ARN ini menyimpan sertifikat publik untuk sertifikat publik portal web Anda. Jika Anda menetapkan nama domain portal untuk sumber daya eksternal otomatis Anda, Anda dapat menemukan nilai ini di bawah tab Output dari tumpukan res-bi.

Parameter	Default	Deskripsi
PrivateKeySecretARNforVDI		(Opsional) Rahasia ARN ini menyimpan kunci pribadi untuk sertifikat portal web Anda. Jika Anda menetapkan nama domain portal untuk sumber daya eksternal otomatis Anda, Anda dapat menemukan nilai ini di bawah tab Output dari tumpukan res-bi.

5. Pilih Membuat tumpukan untuk menerapkannya.

Anda dapat melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda akan menerima status CREATE_COMPLETE dalam waktu sekitar 60 menit.

Langkah 2: Masuk untuk pertama kalinya

Setelah tumpukan produk disebarkan di akun Anda, Anda akan menerima email dengan kredensial Anda. Gunakan URL untuk masuk ke akun Anda dan mengonfigurasi ruang kerja untuk pengguna lain.

Setelah Anda masuk untuk pertama kalinya, Anda dapat mengonfigurasi pengaturan di portal web untuk terhubung ke penyedia SSO. Untuk informasi konfigurasi pasca-penerapan, lihat.

[Panduan konfigurasi](#) Perhatikan bahwa `clusteradmin` ini adalah akun break-glass — Anda dapat menggunakannya untuk membuat proyek dan menetapkan keanggotaan pengguna atau grup untuk proyek-proyek tersebut; itu tidak dapat menetapkan tumpukan perangkat lunak atau menyebarkan desktop untuk dirinya sendiri.

Perbarui produk

Research and Engineering Studio (RES) memiliki dua metode untuk memperbarui produk yang bergantung pada apakah pembaruan versi mayor atau minor.

RES menggunakan skema versi berbasis tanggal. Rilis utama menggunakan tahun dan bulan, dan rilis minor menambahkan nomor urut bila perlu. Misalnya, versi 2024.01 dirilis pada Januari 2024 sebagai rilis utama; versi 2024.01.01 adalah pembaruan rilis kecil dari versi itu.

Topik

- [Pembaruan versi utama](#)
- [Pembaruan versi minor](#)

Pembaruan versi utama

Research and Engineering Studio menggunakan snapshot untuk mendukung migrasi dari lingkungan RES sebelumnya ke yang terbaru tanpa kehilangan pengaturan lingkungan Anda. Anda juga dapat menggunakan proses ini untuk menguji dan memverifikasi pembaruan ke lingkungan Anda sebelum mengarahkan pengguna.

Untuk memperbarui lingkungan Anda dengan RES versi terbaru:

1. Buat snapshot dari lingkungan Anda saat ini. Lihat [the section called “Buat snapshot”](#).
2. Menerapkan ulang RES dengan versi baru. Lihat [the section called “Langkah 1: Luncurkan produk”](#).
3. Terapkan snapshot ke lingkungan Anda yang diperbarui. Lihat [the section called “Terapkan snapshot”](#).
4. Verifikasi semua data yang berhasil dimigrasi ke lingkungan baru.

Pembaruan versi minor

Untuk pembaruan versi minor ke RES, instalasi baru tidak diperlukan. Anda dapat memperbarui tumpukan RES yang ada dengan memperbarui AWS CloudFormation templatnya. Periksa versi lingkungan RES Anda saat ini AWS CloudFormation sebelum menerapkan pembaruan. Anda dapat menemukan nomor versi di awal template.

Misalnya: "Description": "RES_2024.1"

Untuk membuat pembaruan versi minor:

1. Unduh AWS CloudFormation template terbaru di [the section called “Langkah 1: Luncurkan produk”](#).
2. Buka AWS CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
3. Dari Stacks, temukan dan pilih tumpukan utama. Itu harus muncul sebagai *<stack-name>*.
4. Pilih Perbarui.
5. Pilih Ganti template saat ini.
6. Untuk Sumber templat, pilih Unggah file templat.
7. Pilih file dan unggah templat yang Anda unduh.
8. Pada Tentukan detail tumpukan, pilih Berikutnya. Anda tidak perlu memperbarui parameter.
9. Pada opsi Konfigurasi tumpukan, pilih Berikutnya.
10. Pada Review<stack-name>, pilih Submit.

Copot pemasangan produk

Anda dapat menghapus instalasi Studio Penelitian dan Teknik pada AWS produk dari AWS Management Console atau dengan menggunakan AWS Command Line Interface. Anda harus menghapus bucket Amazon Simple Storage Service (Amazon S3) secara manual yang dibuat oleh produk ini. Produk ini tidak secara otomatis menghapus < EnvironmentName >- shared-storage-security-group jika Anda telah menyimpan data untuk disimpan.

Menggunakan AWS Management Console

1. Masuk ke [konsol AWS CloudFormation](#) tersebut.
2. Pada halaman Stacks, pilih tumpukan instalasi produk ini.
3. Pilih Hapus.

Menggunakan AWS Command Line Interface

Tentukan apakah AWS Command Line Interface (AWS CLI) tersedia di lingkungan Anda. Untuk petunjuk penginstalan, lihat [Apa yang ada AWS Command Line Interface](#) di Panduan AWS CLI Pengguna. Setelah mengonfirmasi bahwa AWS CLI tersedia dan dikonfigurasi ke akun administrator di Wilayah tempat produk digunakan, jalankan perintah berikut.

```
$ aws cloudformation delete-stack --stack-name <RES-stack-name>
```

Menghapus shared-storage-security-group

Warning

Produk mempertahankan sistem file ini secara default untuk melindungi terhadap kehilangan data yang tidak disengaja. Jika Anda memilih untuk menghapus grup keamanan dan sistem file terkait, data apa pun yang disimpan dalam sistem tersebut akan dihapus secara permanen. Kami merekomendasikan untuk membuat cadangan data atau menetapkan kembali data ke grup keamanan baru.

1. Masuk ke AWS Management Console dan buka konsol Amazon EFS di <https://console.aws.amazon.com/efs/>.
2. Hapus semua sistem file yang terkait dengan `<RES-stack-name>-shared-storage-security-group`. Atau, Anda dapat menetapkan ulang sistem file ini ke grup keamanan lain untuk memelihara data.
3. Masuk ke AWS Management Console dan buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
4. Hapus `<RES-stack-name>-shared-storage-security-group`.

Menghapus bucket Amazon S3

Produk ini dikonfigurasi untuk mempertahankan bucket Amazon S3 yang dibuat produk (untuk diterapkan di Wilayah keikutsertaan) jika Anda memutuskan untuk menghapus tumpukan untuk mencegah kehilangan data yang tidak AWS CloudFormation disengaja. Setelah mencopot pemasangan produk, Anda dapat menghapus bucket S3 ini secara manual jika Anda tidak perlu menyimpan data. Ikuti langkah-langkah ini untuk menghapus bucket Amazon S3.

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di <https://console.aws.amazon.com/s3/>
2. Pilih Bucket dari panel navigasi.
3. Temukan ember `stack-name S3`.
4. Pilih setiap bucket Amazon S3, lalu pilih Kosong. Anda harus mengosongkan setiap ember.
5. Pilih bucket S3 dan pilih Delete.

Untuk menghapus bucket S3 menggunakan AWS CLI, jalankan perintah berikut:

```
$ aws s3 rb s3://<bucket-name> --force
```

Note

`--force` Perintah mengosongkan ember isinya.

Panduan konfigurasi

Panduan konfigurasi ini memberikan instruksi pasca-penerapan untuk audiens teknis tentang cara menyesuaikan dan mengintegrasikan lebih lanjut dengan Studio Penelitian dan Teknik pada AWS produk.

Topik

- [Manajemen identitas](#)
- [Membuat subdomain](#)
- [Buat sertifikat ACM](#)
- [CloudWatch Log Amazon](#)
- [Menetapkan batas izin khusus](#)
- [Konfigurasi RES-Ready AMLs](#)

Manajemen identitas

Research and Engineering Studio dapat menggunakan penyedia identitas yang sesuai dengan SAMP 2.0. Untuk menggunakan Amazon Cognito sebagai direktori pengguna asli yang memungkinkan pengguna masuk ke portal Web dan berbasis Linux dengan identitas pengguna VDLs Cognito, lihat. [Menyiapkan pengguna Amazon Cognito](#) Jika Anda menerapkan RES menggunakan sumber daya eksternal atau berencana menggunakan Pusat Identitas IAM, lihat. [Menyiapkan sistem masuk tunggal \(SSO\) dengan IAM Identity Center](#) Jika Anda memiliki penyedia identitas yang sesuai dengan SAMP 2.0 Anda sendiri, lihat. [Mengkonfigurasi penyedia identitas Anda untuk single sign-on \(SSO\)](#)

Topik

- [Menyiapkan pengguna Amazon Cognito](#)
- [Sinkronisasi Direktori Aktif](#)
- [Menyiapkan sistem masuk tunggal \(SSO\) dengan IAM Identity Center](#)
- [Mengkonfigurasi penyedia identitas Anda untuk single sign-on \(SSO\)](#)
- [Mengatur kata sandi untuk pengguna](#)

Menyiapkan pengguna Amazon Cognito

Research and Engineering Studio (RES) memungkinkan Anda mengatur Amazon Cognito sebagai direktori pengguna asli. Ini memungkinkan pengguna untuk masuk ke portal web dan berbasis Linux dengan identitas pengguna Amazon VDI's Cognito. Administrator dapat mengimpor beberapa pengguna ke kumpulan pengguna menggunakan file csv dari AWS Konsol. Untuk detail selengkapnya tentang impor pengguna massal, lihat [Mengimpor pengguna ke kumpulan pengguna dari file CSV](#) di Panduan Pengembang Amazon Cognito. RES mendukung penggunaan direktori pengguna asli berbasis Amazon Cognito dan SSO bersama-sama.

Pengaturan administratif

Sebagai Administrator RES, untuk mengonfigurasi lingkungan RES agar menggunakan Amazon Cognito sebagai direktori pengguna, alihkan tombol Gunakan Amazon Cognito sebagai direktori pengguna di halaman Manajemen Identitas yang dapat diakses dari halaman Manajemen Lingkungan. Untuk memungkinkan pengguna mendaftar sendiri, alihkan tombol registrasi mandiri Pengguna di halaman yang sama.

Alur up/sign masuk pengguna

Jika registrasi mandiri Pengguna diaktifkan, Anda dapat memberikan URL aplikasi web kepada pengguna Anda. Di sana, pengguna akan menemukan opsi yang mengatakan Belum pengguna? Daftar di sini.

Alur daftar

Pengguna yang memilih Belum menjadi pengguna? Mendaftar di sini akan diminta untuk memasukkan email dan kata sandi mereka untuk membuat akun.

Sebagai bagian dari alur pendaftaran, pengguna akan diminta untuk memasukkan kode verifikasi yang diterima di email mereka untuk menyelesaikan proses pendaftaran.

Jika pendaftaran mandiri dinonaktifkan, pengguna tidak akan melihat tautan pendaftaran. Administrator harus mengonfigurasi pengguna di Amazon Cognito di luar RES. (Lihat [Membuat akun pengguna sebagai administrator](#) di Panduan Pengembang Amazon Cognito.)

Halaman Login Pilihan

Jika SSO dan Amazon Cognito diaktifkan, opsi untuk Masuk dengan organisasi SSO akan muncul. Ketika pengguna mengklik opsi itu, itu akan mengalihkan mereka ke halaman login SSO mereka. Secara default, pengguna akan mengautentikasi dengan Amazon Cognito jika diaktifkan.

Batasan

- Nama Grup Amazon Cognito Anda dapat memiliki maksimal enam huruf; hanya huruf kecil yang diterima.
- Pendaftaran Amazon Cognito tidak akan mengizinkan dua alamat email dengan nama pengguna yang sama tetapi alamat domain yang berbeda.
- Jika Active Directory dan Amazon Cognito diaktifkan, dan sistem mendeteksi nama pengguna duplikat, hanya pengguna Active Directory yang diizinkan untuk mengautentikasi. Administrator harus mengambil langkah-langkah untuk tidak mengonfigurasi nama pengguna duplikat antara Amazon Cognito dan Direktori Aktif mereka.
- Pengguna Cognito tidak akan diizinkan untuk meluncurkan berbasis Windows VDIs karena RES tidak mendukung otentikasi berbasis Amazon Cognito untuk instance Windows.

Sinkronisasi

RES menyinkronkan database-nya dengan informasi pengguna dan grup dari Amazon Cognito setiap jam. Setiap pengguna yang termasuk dalam grup “admin” akan diberikan hak istimewa sudo di dalamnya. VDIs

Anda juga dapat memulai sinkronisasi secara manual dari konsol Lambda.

Memulai proses sinkronisasi secara manual:

1. Buka [Konsol Lambda](#).
2. Cari Lambda sinkronisasi Cognito. Lambda ini mengikuti konvensi penamaan ini: `{RES_ENVIRONMENT_NAME}_cognito-sync-lambda`
3. Pilih Uji.
4. Di bagian Test event, pilih tombol Test di kanan atas. Format badan acara tidak masalah.

Pertimbangan keamanan untuk Cognito

Sebelum rilis 2024.12, [pencatatan aktivitas pengguna](#), yang merupakan bagian dari fitur paket Amazon Cognito Plus diaktifkan secara default. Kami menghapus ini dari penerapan dasar kami untuk menghemat biaya bagi pelanggan yang ingin mencoba RES. Anda dapat mengaktifkan kembali fitur ini sesuai kebutuhan untuk menyelaraskan dengan pengaturan keamanan cloud organisasi Anda.

Sinkronisasi Direktori Aktif

Konfigurasi Runtime

Semua parameter CFN yang terkait dengan Active Directory (AD) bersifat opsional selama instalasi.

Setelah instalasi awal, administrator dapat melihat atau mengedit konfigurasi AD di portal web RES di bawah halaman Manajemen identitas:

Administrator dapat memfilter pengguna atau grup untuk disinkronkan melalui opsi Filter Pengguna dan Filter Grup yang baru. Filter harus mengikuti [sintaks filter LDAP](#). Contoh filter adalah:

```
(sAMAccountname=<user>)
```

Untuk ARN rahasia apa pun yang disediakan saat runtime (misalnya, `ServiceAccountCredentialsSecretArn` atau `DomainTLSCertificateSecretArn`), pastikan untuk menambahkan tag berikut ke rahasia untuk RES untuk mendapatkan izin membaca nilai rahasia:

- kunci:res:EnvironmentName, nilai: *<your RES environment name>*
- kunci:res:ModuleName, nilai: `directoryservice`

Setiap pembaruan konfigurasi AD di portal web akan diambil secara otomatis selama sinkronisasi AD terjadwal berikutnya (per jam). Pengguna mungkin perlu mengkonfigurasi ulang SSO setelah mengubah konfigurasi AD (misalnya, jika mereka beralih ke AD yang berbeda).

Cara menjalankan sinkronisasi secara manual (rilis 2024.12 dan yang lebih baru)

Proses sinkronisasi Direktori Aktif telah dipindahkan dari host infra Manajer Cluster ke tugas Amazon Elastic Container Service (ECS) satu kali di belakang layar. Proses ini dijadwalkan untuk berjalan setiap jam dan Anda dapat menemukan tugas ECS yang sedang berjalan di konsol Amazon ECS di bawah `<res-environment-name>-ad-sync-cluster` cluster saat sedang berlangsung.

Untuk meluncurkannya secara manual:

1. Arahkan ke [konsol Lambda](#) dan cari lambda yang dipanggil. `<res-environment>-scheduled-ad-sync`
2. Buka fungsi Lambda dan pergi ke Test
3. Dalam Acara JSON masukkan yang berikut ini:

```
{
  "detail-type": "Scheduled Event"
}
```

4. Pilih Uji.
5. Amati log tugas AD Sync yang sedang berjalan di bawah CloudWatch→ Grup Log → `<environment-name>/ad-sync`. Anda akan melihat log dari masing-masing tugas ECS yang sedang berjalan. Pilih yang terbaru untuk melihat log.

Note

- Jika Anda mengubah parameter AD atau menambahkan filter AD, RES akan menambahkan pengguna baru dengan parameter yang baru ditentukan dan menghapus pengguna yang sebelumnya disinkronkan dan tidak lagi disertakan dalam ruang pencarian LDAP.
- RES tidak dapat menghapus user/group yang secara aktif ditugaskan ke proyek. Anda harus menghapus pengguna dari proyek agar RES menghapusnya dari lingkungan.

Konfigurasi SSO

Setelah konfigurasi AD disediakan, pengguna harus menyiapkan Single Sign-On (SSO) untuk dapat masuk ke portal web RES sebagai pengguna AD. Konfigurasi SSO telah dipindahkan dari halaman

Pengaturan Umum ke halaman manajemen Identitas baru. Untuk informasi selengkapnya tentang pengaturan SSO, lihat [Manajemen identitas](#).

Menyiapkan sistem masuk tunggal (SSO) dengan IAM Identity Center

Jika Anda belum memiliki pusat identitas yang terhubung ke Direktori Aktif yang dikelola, mulailah dengan [Langkah 1: Siapkan pusat identitas](#). Jika Anda sudah memiliki pusat identitas yang terhubung dengan Direktori Aktif yang dikelola, mulailah dengan [Langkah 2: Connect ke pusat identitas](#).

Note

Jika Anda menyebarkan ke Wilayah AWS GovCloud (AS-Barat), siapkan SSO di akun AWS GovCloud (US) partisi tempat Anda menggunakan Research and Engineering Studio.

Langkah 1: Siapkan pusat identitas

Mengaktifkan Pusat Identitas IAM

1. Masuk ke [konsol AWS Identity and Access Management](#) tersebut.
2. Buka Pusat Identitas.
3. Pilih Aktifkan.
4. Pilih Aktifkan dengan AWS Organizations.
5. Pilih Lanjutkan.

Note

Pastikan Anda berada di Wilayah yang sama di mana Anda memiliki Direktori Aktif terkelola.

Menghubungkan Pusat Identitas IAM ke Direktori Aktif yang dikelola

Setelah Anda mengaktifkan Pusat Identitas IAM, selesaikan langkah-langkah pengaturan yang disarankan ini:

1. Pada panel navigasi, silakan pilih Pengaturan.
2. Di bawah Sumber identitas, pilih Tindakan dan pilih Ubah sumber identitas.

3. Di bawah Direktori yang ada, pilih direktori Anda.
4. Pilih Berikutnya.
5. Tinjau perubahan Anda dan masukkan **ACCEPT** di kotak konfirmasi.
6. Pilih Ubah sumber identitas.

Menyinkronkan pengguna dan grup ke pusat identitas

Setelah perubahan yang dilakukan [Menghubungkan Pusat Identitas IAM ke Direktori Aktif yang dikelola](#) selesai, spanduk konfirmasi hijau muncul.

1. Di spanduk konfirmasi, pilih Mulai penyiapan yang dipandu.
2. Dari Konfigurasi pemetaan atribut, pilih Berikutnya.
3. Di bawah bagian Pengguna, masukkan pengguna yang ingin Anda sinkronkan.
4. Pilih Tambahkan.
5. Pilih Berikutnya.
6. Tinjau perubahan Anda, lalu pilih Simpan konfigurasi.
7. Proses sinkronisasi mungkin memakan waktu beberapa menit. Jika Anda menerima pesan peringatan tentang pengguna yang tidak menyinkronkan, pilih Lanjutkan sinkronisasi.

Mengaktifkan pengguna

1. Dari menu, pilih Pengguna.
2. Pilih pengguna yang ingin Anda aktifkan aksesnya.
3. Pilih Aktifkan akses pengguna.

Langkah 2: Connect ke pusat identitas

Menyiapkan aplikasi di IAM Identity Center

1. Buka [konsol Pusat Identitas IAM](#).
2. Pilih Aplikasi.
3. Pilih Tambahkan aplikasi.
4. Di bawah preferensi Pengaturan, pilih Saya memiliki aplikasi yang ingin saya atur.
5. Di bawah Jenis aplikasi, pilih SAMP 2.0.

6. Pilih Berikutnya.
7. Masukkan nama tampilan dan deskripsi yang ingin Anda gunakan.
8. Di bawah metadata IAM Identity Center, salin tautan untuk file metadata SAM Identity Center IAM. Anda akan memerlukan ini saat mengonfigurasi Pusat Identitas IAM dengan portal RES.
9. Di bawah Properti aplikasi, masukkan URL mulai Aplikasi Anda. Misalnya, `<your-portal-domain>/sso`.
10. Di bawah URL ACS Aplikasi, masukkan URL pengalihan dari portal RES. Untuk menemukan ini:
 - a. Di bawah Manajemen lingkungan, pilih Pengaturan umum.
 - b. Pilih tab Penyedia identitas.
 - c. Di bawah Single Sign-On, Anda akan menemukan URL Pengalihan SAMP.
11. Di bawah Audiens SAMP Aplikasi, masukkan Amazon Cognito URN.

Untuk membuat guci:

- a. Dari portal RES, buka Pengaturan Umum.
- b. Di bawah tab Penyedia identitas, cari ID Kumpulan Pengguna.
- c. Tambahkan ID User Pool ke string ini:

```
urn:amazon:cognito:sp:<user_pool_id>
```

12. Setelah Anda memasukkan Amazon Cognito URN, pilih Kirim.

Mengkonfigurasi pemetaan atribut untuk aplikasi

1. Dari Pusat Identitas, buka detail untuk aplikasi yang Anda buat.
2. Pilih Tindakan, lalu pilih Edit pemetaan atribut.
3. Di bawah Subjek, masukkan `${user:email}`.
4. Di bawah Format, pilih EmailAddress.
5. Pilih Tambahkan pemetaan atribut baru.
6. Di bawah atribut Pengguna dalam aplikasi, masukkan 'email'.
7. Di bawah Peta ke nilai string ini atau atribut pengguna di Pusat Identitas IAM, masukkan `${user:email}`.
8. Di bawah Format, masukkan 'tidak ditentukan'.
9. Pilih Simpan perubahan.

Menambahkan pengguna ke aplikasi di IAM Identity Center

1. Dari Pusat Identitas, buka Pengguna yang Ditugaskan untuk aplikasi yang Anda buat dan pilih Tetapkan pengguna.
2. Pilih pengguna yang ingin Anda tetapkan akses aplikasi.
3. Pilih Tetapkan pengguna.

Menyiapkan Pusat Identitas IAM dalam lingkungan RES

1. Dari lingkungan Studio Penelitian dan Teknik, di bawah manajemen Lingkungan, buka Pengaturan umum.
2. Buka tab Penyedia identitas.
3. Di bawah Single Sign-On, pilih Edit (di samping Status).
4. Lengkapi formulir dengan informasi berikut:
 - a. Pilih SAML.
 - b. Di bawah nama Penyedia, masukkan nama yang ramah pengguna.
 - c. Pilih Masukkan URL titik akhir dokumen metadata.
 - d. Masukkan URL yang Anda salin selama [Menyiapkan aplikasi di IAM Identity Center](#).
 - e. Di bawah atribut email Penyedia, masukkan 'email'.
 - f. Pilih Kirim.
5. Segarkan halaman dan periksa apakah Status ditampilkan sebagai diaktifkan.

Mengkonfigurasi penyedia identitas Anda untuk single sign-on (SSO)

Research and Engineering Studio terintegrasi dengan penyedia identitas SAMP 2.0 untuk mengautentikasi akses pengguna ke portal RES. Langkah-langkah ini memberikan petunjuk untuk berintegrasi dengan penyedia identitas SAMP 2.0 pilihan Anda. Jika Anda berniat menggunakan IAM Identity Center, silakan lihat [Menyiapkan sistem masuk tunggal \(SSO\) dengan IAM Identity Center](#).

Note

Email pengguna harus cocok dengan pernyataan IDP SAMP dan Active Directory. Anda harus menghubungkan penyedia identitas Anda dengan Active Directory Anda dan menyinkronkan pengguna secara berkala.

Topik

- [Konfigurasi penyedia identitas Anda](#)
- [Konfigurasi RES untuk menggunakan penyedia identitas Anda](#)
- [Mengkonfigurasi penyedia identitas Anda di lingkungan non-produksi](#)
- [Debugging masalah SAMP iDP](#)

Konfigurasi penyedia identitas Anda

Bagian ini menyediakan langkah-langkah untuk mengonfigurasi penyedia identitas Anda dengan informasi dari kumpulan pengguna Amazon Cognito RES.

1. RES mengasumsikan bahwa Anda memiliki AD (AWS Managed AD atau iklan yang disediakan sendiri) dengan identitas pengguna yang diizinkan untuk mengakses portal dan proyek RES. Hubungkan iklan Anda ke penyedia layanan identitas Anda dan sinkronkan identitas pengguna. Periksa dokumentasi penyedia identitas Anda untuk mempelajari cara menghubungkan AD dan menyinkronkan identitas pengguna. Misalnya, lihat [Menggunakan Active Directory sebagai sumber identitas](#) di Panduan AWS IAM Identity Center Pengguna.
2. Konfigurasi aplikasi SAMP 2.0 untuk RES di penyedia identitas Anda (iDP). Konfigurasi ini membutuhkan parameter berikut:
 - URL Pengalihan SAMP — URL yang digunakan IDP Anda untuk mengirim respons SAMP 2.0 ke penyedia layanan.

Note

Bergantung pada IDP, URL Pengalihan SAMP mungkin memiliki nama yang berbeda:

- URL Aplikasi
- URL Pernyataan Layanan Konsumen (ACS)
- URL Pengikatan POST ACS

Untuk mendapatkan URL

1. Masuk ke RES sebagai admin atau clusteradmin.
2. Arahkan ke Manajemen Lingkungan ⇒ Pengaturan Umum ⇒ Penyedia Identitas.
3. Pilih URL Pengalihan SAMP.

- SAMP Audience URI — ID unik dari entitas audiens SAMP di sisi penyedia layanan.

 Note

Bergantung pada IDP, URI Audiens SAMP mungkin memiliki nama yang berbeda:

- ClientID
- Aplikasi SAMP Audiens
- ID entitas SP

Berikan masukan dalam format berikut.

```
urn:amazon:cognito:sp:user-pool-id
```

Untuk menemukan URI Audiens SAMP

1. Masuk ke RES sebagai admin atau clusteradmin.
 2. Arahkan ke Manajemen Lingkungan ⇒ Pengaturan Umum ⇒ Penyedia Identitas.
 3. Pilih User Pool Id.
3. Pernyataan SAMP yang diposting ke RES harus memiliki fields/claims set berikut ke alamat email pengguna:
- Subjek SAMP atau NameID
 - Email SAMP
4. IDP Anda fields/claims menambah pernyataan SAMP, berdasarkan konfigurasi. RES membutuhkan bidang ini. Sebagian besar penyedia secara otomatis mengisi bidang ini secara default. Lihat input dan nilai bidang berikut jika Anda harus mengonfigurasinya.
- AudienceRestriction — Atur ke `urn:amazon:cognito:sp:user-pool-id`. Ganti *user-pool-id* dengan ID kumpulan pengguna Amazon Cognito Anda.

```
<saml:AudienceRestriction>  
  <saml:Audience> urn:amazon:cognito:sp:user-pool-id  
</saml:AudienceRestriction>
```

- Respons - Setel InResponseTo ke `https://user-pool-domain/saml2/idpresponse`. Ganti *user-pool-domain* dengan nama domain kumpulan pengguna Amazon Cognito Anda.

```
<saml2p:Response
  Destination="http://user-pool-domain/saml2/idpresponse"
  ID="id123"
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  IssueInstant="Date-time stamp"
  Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

- SubjectConfirmationData— Setel Recipient ke `saml2/idpresponse` titik akhir kumpulan pengguna Anda dan InResponseTo ke ID permintaan SAMP asli.

```
<saml2:SubjectConfirmationData
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  NotOnOrAfter="Date-time stamp"
  Recipient="https://user-pool-domain/saml2/idpresponse"/>
```

- AuthnStatement— Konfigurasi sebagai berikut:

```
<saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ"
  SessionIndex="32413b2e54db89c764fb96ya2k"
  SessionNotOnOrAfter="2016-10-30T13:13:28">
  <saml2:SubjectLocality />
  <saml2:AuthnContext>

  <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
```

5. Jika aplikasi SAMP Anda memiliki bidang URL logout, atur ke: `<domain-url>/saml2/logout`

Untuk mendapatkan URL domain

1. Masuk ke RES sebagai admin atau clusteradmin.
2. Arahkan ke Manajemen Lingkungan ⇒ Pengaturan Umum ⇒ Penyedia Identitas.

3. Pilih URL Domain.
6. Jika IDP Anda menerima sertifikat penandatanganan untuk membangun kepercayaan dengan Amazon Cognito, unduh sertifikat penandatanganan Amazon Cognito dan unggah di IDP Anda.

Untuk mendapatkan sertifikat penandatanganan

1. Buka konsol Amazon Cognito di [Memulai](#) dengan AWS Management Console
2. Pilih kumpulan pengguna Anda. Kumpulan pengguna Anda seharusnya `<environment name>-user-pool`.
3. Pilih tab Pengalaman masuk.
4. Di bagian login penyedia identitas terfederasi, pilih Lihat sertifikat penandatanganan.

Anda dapat menggunakan sertifikat ini untuk menyiapkan IDP Direktori Aktif, menambahkan `relying party trust`, dan mengaktifkan dukungan SAMP pada pihak yang mengandalkannya ini.



Note

Ini tidak berlaku untuk Keycloak dan IDC.

5. Setelah pengaturan aplikasi selesai, unduh metadata aplikasi SAMP 2.0 XML/URL. Anda menggunakannya di bagian selanjutnya.

Konfigurasi RES untuk menggunakan penyedia identitas Anda

Untuk menyelesaikan pengaturan sistem masuk tunggal untuk RES

1. Masuk ke RES sebagai admin atau clusteradmin.
2. Arahkan ke Manajemen Lingkungan $\Rightarrow$ Pengaturan Umum $\Rightarrow$ Penyedia Identitas.
3. Di bawah Single Sign-On, pilih ikon edit di sebelah indikator status untuk membuka halaman Single Sign On Configuration.

- a. Untuk Penyedia Identitas, pilih SAMP.
- b. Untuk Nama Penyedia, masukkan nama unik untuk penyedia identitas Anda.

 Note

Nama-nama berikut tidak diperbolehkan:

- Cognito
- IdentityCenter

- c. Di bawah Sumber Dokumen Metadata, pilih opsi yang sesuai dan unggah dokumen XMLmetadata atau berikan URL dari penyedia identitas.
 - d. Untuk Atribut Email Penyedia, masukkan nilai `teksemail`.
 - e. Pilih Kirim.
4. Muat ulang halaman Pengaturan Lingkungan. Single sign-on diaktifkan jika konfigurasi sudah benar.

Mengkonfigurasi penyedia identitas Anda di lingkungan non-produksi

Jika Anda menggunakan [sumber daya eksternal](#) yang disediakan untuk membuat lingkungan RES non-produksi dan mengonfigurasi Pusat Identitas IAM sebagai penyedia identitas Anda, Anda mungkin ingin mengonfigurasi penyedia identitas yang berbeda seperti Okta. Formulir pemberdayaan RES SSO meminta tiga parameter konfigurasi:

1. Nama penyedia - Tidak dapat diubah
2. Dokumen metadata atau URL — Dapat dimodifikasi
3. Atribut email penyedia - Dapat dimodifikasi

Untuk mengubah dokumen metadata dan atribut email penyedia, lakukan hal berikut:

1. Masuk ke Konsol Amazon Cognito.
2. Dari navigasi, pilih Kumpulan pengguna.
3. Pilih kumpulan pengguna Anda untuk melihat ikhtisar kumpulan Pengguna.
4. Dari tab Pengalaman masuk, buka login penyedia identitas Federasi dan buka penyedia identitas Anda yang dikonfigurasi.

5. Umumnya, Anda hanya akan diminta untuk mengubah metadata dan membiarkan pemetaan atribut tidak berubah. Untuk memperbarui pemetaan Atribut, pilih Edit. Untuk memperbarui dokumen Metadata, pilih Ganti metadata.
6. Jika Anda mengedit pemetaan atribut, Anda perlu memperbarui `<environment name>.cluster-settings` tabel di DynamoDB.
 - a. Buka konsol DynamoDB dan pilih Tabel dari navigasi.
 - b. Temukan dan pilih `<environment name>.cluster-settings` tabel, dan dari menu Tindakan pilih Jelajahi item.
 - c. Di bawah Pindai atau kueri item, buka Filter dan masukkan parameter berikut:
 - Nama atribut — key
 - Nilai - `identity-provider.cognito.sso_idp_provider_email_attribute`
 - d. Pilih Jalankan.
7. Di bawah Item yang dikembalikan, temukan `identity-provider.cognito.sso_idp_provider_email_attribute` string dan pilih Edit untuk memodifikasi string agar sesuai dengan perubahan Anda di Amazon Cognito.

Debugging masalah SAMP IDP

SAML-tracer - Anda dapat menggunakan ekstensi ini untuk browser Chrome untuk melacak permintaan SAMP dan memeriksa nilai pernyataan SAMP. Untuk informasi selengkapnya, lihat [SAML-tracer](#) di toko web Chrome.

Alat pengembang SAMP - OneLogin menyediakan alat yang dapat Anda gunakan untuk memecahkan kode nilai yang dikodekan SAMP dan memeriksa bidang yang diperlukan dalam pernyataan SAMP. Untuk informasi lebih lanjut, lihat [Base 64 Decode+Inflate](#) di OneLogin situs web.

Amazon CloudWatch Logs — Anda dapat memeriksa log RES Anda di CloudWatch Log untuk kesalahan atau peringatan. Log Anda berada dalam grup log dengan format nama `res-environment-name/cluster-manager`.

Dokumentasi Amazon Cognito — Untuk informasi selengkapnya tentang integrasi SAMP dengan Amazon Cognito, lihat [Menambahkan penyedia identitas SAMP ke kumpulan pengguna di Panduan Pengembang](#) Amazon Cognito.

Mengatur kata sandi untuk pengguna

1. Dari [AWS Directory Service konsol](#), pilih direktori untuk tumpukan yang dibuat.
2. Di bawah menu Tindakan, pilih Setel ulang kata sandi pengguna.
3. Pilih pengguna dan masukkan kata sandi baru.
4. Pilih Setel ulang kata sandi.

Membuat subdomain

Jika Anda menggunakan domain khusus, Anda perlu mengatur subdomain untuk mendukung bagian web dan VDI portal Anda.

Note

Jika Anda menyebarkan ke Wilayah AWS GovCloud (AS-Barat), siapkan aplikasi web dan subdomain VDI di akun partisi komersial yang menghosting zona domain yang dihosting publik.

1. Buka [konsol Route 53](#).
2. Temukan domain yang Anda buat dan pilih Buat catatan.
3. Masukkan 'web' sebagai nama Rekam.
4. Pilih CNAME sebagai tipe Rekam.
5. Untuk Nilai, masukkan tautan yang Anda terima di email awal.
6. Pilih Create records (Buat catatan).
7. Untuk membuat catatan untuk VDC, ambil alamat NLB.
 - a. Buka [konsol AWS CloudFormation](#).
 - b. Pilih <environment-name>-vdc.
 - c. Pilih Sumber Daya dan buka <environmentname>-vdc-external-nlb.
 - d. Salin nama DNS dari NLB.
8. Buka [konsol Route 53](#).
9. Temukan domain Anda dan pilih Buat catatan.
10. Di bawah nama Rekam, masukkan vdc.

11. Di bawah Jenis rekaman, pilih CNAME.
12. Untuk NLB, masukkan DNS.
13. Pilih Buat catatan.

Buat sertifikat ACM

Secara default, RES meng-host portal web di bawah penyeimbang beban aplikasi menggunakan domain amazonaws.com. Untuk menggunakan domain Anda sendiri, Anda perlu mengonfigurasi SSL/TLS sertifikat publik yang disediakan oleh Anda atau diminta dari AWS Certificate Manager (ACM). Jika Anda menggunakan ACM, Anda akan menerima nama AWS sumber daya yang perlu Anda berikan sebagai parameter untuk mengenkripsi SSL/TLS saluran antara klien dan host layanan web.

Tip

Jika Anda menerapkan paket demo sumber daya eksternal, Anda harus memasukkan domain yang Anda pilih `PortalDomainName` saat menerapkan tumpukan sumber daya eksternal. [Buat sumber daya eksternal](#)

Untuk membuat sertifikat untuk domain kustom:

1. Dari konsol, buka [AWS Certificate Manager](#) untuk meminta sertifikat publik. Jika Anda menerapkan di AWS GovCloud (AS-Barat), buat sertifikat di akun GovCloud partisi Anda.
2. Pilih Minta sertifikat publik, dan pilih Berikutnya.
3. Di bawah nama Domain, minta sertifikat untuk keduanya `*.PortalDomainName` dan `PortalDomainName`.
4. Di bawah metode Validasi, pilih validasi DNS.
5. Pilih Minta.
6. Dari daftar Sertifikat, buka sertifikat yang Anda minta. Setiap sertifikat akan memiliki validasi Tertunda sebagai status.

Note

Jika Anda tidak melihat sertifikat Anda, segarkan daftar.

7. Lakukan salah satu tindakan berikut:

- Penyebaran komersial:

Dari detail Sertifikat untuk setiap sertifikat yang diminta, pilih Buat catatan di Rute 53. Status sertifikat harus berubah menjadi Diterbitkan.

- GovCloud penyebaran:

Jika Anda menerapkan di AWS GovCloud (AS-Barat), salin kunci dan nilai CNAME. Dari akun partisi komersial, gunakan nilai untuk membuat catatan baru di Zona Hosted Publik. Status sertifikat harus berubah menjadi Diterbitkan.

8. Salin sertifikat ARN baru untuk dimasukkan sebagai parameter untuk.

ACMCertificateARNforWebApp

CloudWatch Log Amazon

Research and Engineering Studio membuat grup log berikut CloudWatch selama instalasi. Lihat tabel berikut untuk retensi default:

CloudWatch Grup log	Penyimpanan
/aws/lambda/ <i><installation-stack-name></i> -cluster-endpoints	Tidak pernah kedaluwarsa
/aws/lambda/ <i><installation-stack-name></i> -cluster-manager-scheduled-ad-sync	Tidak pernah kedaluwarsa
/aws/lambda/ <i><installation-stack-name></i> -cluster-settings	Tidak pernah kedaluwarsa
/aws/lambda/ <i><installation-stack-name></i> -oauth-credentials	Tidak pernah kedaluwarsa
/aws/lambda/ <i><installation-stack-name></i> -self-signed-certificate	Tidak pernah kedaluwarsa

CloudWatch Grup log	Penyimpanan
<code>/aws/lambda/ <installation-stack-name>-update-cluster-prefix-list</code>	Tidak pernah kedaluwarsa
<code>/aws/lambda/ <installation-stack-name>-vdc-scheduled-event-transformer</code>	Tidak pernah kedaluwarsa
<code>/aws/lambda/ <installation-stack-name>-vdc-update-cluster-manager-client-scope</code>	Tidak pernah kedaluwarsa
<code>/<installation-stack-name> /cluster-manager</code>	3 bulan
<code>/<installation-stack-name> /vdc/controller</code>	3 bulan
<code>/<installation-stack-name> /vdc/dcv-broker</code>	3 bulan
<code>/<installation-stack-name> /vdc/dcv-connection-gateway</code>	3 bulan

Jika Anda ingin mengubah retensi default untuk grup log, Anda dapat pergi ke [CloudWatch konsol](#) dan mengikuti petunjuk untuk [Mengubah penyimpanan data CloudWatch log di Log](#).

Menetapkan batas izin khusus

Mulai 2024.04, Anda dapat secara opsional memodifikasi peran yang dibuat oleh RES dengan melampirkan batas izin khusus. Batas izin khusus dapat didefinisikan sebagai bagian dari AWS CloudFormation instalasi RES dengan memberikan ARN batas izin sebagai bagian dari parameter Batas. IAMPermission Tidak ada batas izin yang ditetapkan pada peran RES apa pun jika parameter ini dibiarkan kosong. Di bawah ini adalah daftar tindakan yang diperlukan peran RES untuk beroperasi. Pastikan bahwa batas izin apa pun yang Anda rencanakan untuk digunakan secara eksplisit memungkinkan tindakan berikut:

```
[
  {
    "Effect": "Allow",
    "Resource": "*",
    "Sid": "ResRequiredActions",
    "Action": [
      "access-analyzer:*",
      "account:GetAccountInformation",
      "account:ListRegions",
      "acm:*",
      "airflow:*",
      "amplify:*",
      "amplifybackend:*",
      "amplifyuibuilder:*",
      "aoss:*",
      "apigateway:*",
      "appflow:*",
      "application-autoscaling:*",
      "appmesh:*",
      "apprunner:*",
      "aps:*",
      "athena:*",
      "auditmanager:*",
      "autoscaling-plans:*",
      "autoscaling:*",
      "backup-gateway:*",
      "backup-storage:*",
      "backup:*",
      "batch:*",
      "bedrock:*",
      "budgets:*",
      "ce:*",
      "cloud9:*",
      "cloudformation:*",
      "cloudfront:*",
      "cloudtrail-data:*",
      "cloudtrail:*",
      "cloudwatch:*",
      "codeartifact:*",
      "codebuild:*",
      "codeguru-profiler:*",
      "codeguru-reviewer:*",
      "codepipeline:*
```

```
"codestar-connections:*",
"codestar-notifications:*",
"codestar:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"comprehend:*",
"compute-optimizer:*",
"cur:*",
"databrew:*",
"datapipeline:*",
"datasync:*",
"dax:*",
"detective:*",
"devops-guru:*",
"dlm:*",
"dms:*",
"drs:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr:*",
"ecs:*",
"eks:*",
"elastic-inference:*",
"elasticache:*",
"elasticbeanstalk:*",
"elasticfilesystem:*",
"elasticloadbalancing:*",
"elasticmapreduce:*",
"elastictranscoder:*",
"es:*",
"events:*",
"firehose:*",
"fis:*",
"fms:*",
"forecast:*",
"fsx:*",
"geo:*",
"glacier:*",
"glue:*",
"grafana:*,
```

```
"guardduty:*",
"health:*",
"iam:*",
"identitystore:*",
"imagebuilder:*",
"inspector2:*",
"inspector:*",
"internetmonitor:*",
"iot:*",
"iotanalytics:*",
"kafka:*",
"kafkaconnect:*",
"kinesis:*",
"kinesisanalytics:*",
"kms:*",
"lambda:*",
"lightsail:*",
"logs:*",
"memorydb:*",
"mgh:*",
"mobiletargeting:*",
"mq:*",
"neptune-db:*",
"organizations:DescribeOrganization",
"osis:*",
"personalize:*",
"pi:*",
"pipes:*",
"polly:*",
"qldb:*",
"quicksight:*",
"rds-data:*",
"rds:*",
"redshift-data:*",
"redshift-serverless:*",
"redshift:*",
"rekognition:*",
"resiliencehub:*",
"resource-groups:*",
"route53:*",
"route53domains:*",
"route53resolver:*",
"rum:*",
"s3:*,
```

```

    "sagemaker:*",
    "scheduler:*",
    "schemas:*",
    "sdb:*",
    "secretsmanager:*",
    "securityhub:*",
    "serverlessrepo:*",
    "servicecatalog:*",
    "servicequotas:*",
    "ses:*",
    "signer:*",
    "sns:*",
    "sqs:*",
    "ssm:*",
    "ssmmessages:*",
    "states:*",
    "storagegateway:*",
    "sts:*",
    "support:*",
    "tag:GetResources",
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "textract:*",
    "timestream:*",
    "transcribe:*",
    "transfer:*",
    "translate:*",
    "vpc-lattice:*",
    "waf-regional:*",
    "waf:*",
    "wafv2:*",
    "wellarchitected:*",
    "wisdom:*",
    "xray:*"
  ]
}
]

```

Konfigurasi RES-Ready AMIs

Dengan Amazon Machine Images (AMIs) yang siap untuk RES, Anda dapat melakukan pra-instal dependensi RES untuk instans desktop virtual () pada kustom Anda. VDI AMIs Menggunakan

RES-ready, AMIs tingkatkan waktu boot untuk instance VDI menggunakan gambar yang sudah dipanggang sebelumnya. Menggunakan EC2 Image Builder, Anda dapat membangun dan mendaftarkan Anda AMIs sebagai tumpukan perangkat lunak baru. Untuk informasi selengkapnya tentang Image Builder, lihat [Panduan Pengguna Image Builder](#).

Sebelum Anda mulai, Anda harus [menerapkan versi terbaru dari RES](#).

Topik

- [Siapkan peran IAM untuk mengakses lingkungan RES](#)
- [Buat komponen EC2 Image Builder](#)
- [Siapkan resep EC2 Image Builder Anda](#)
- [Konfigurasi infrastruktur EC2 Image Builder](#)
- [Konfigurasi pipa gambar Image Builder](#)
- [Jalankan pipa gambar Image Builder](#)
- [Daftarkan tumpukan perangkat lunak baru di RES](#)

Siapkan peran IAM untuk mengakses lingkungan RES

Untuk mengakses layanan lingkungan RES dari EC2 Image Builder, Anda harus membuat atau memodifikasi peran IAM yang disebut RES- EC2InstanceProfileForImageBuilder. Untuk informasi tentang mengonfigurasi peran IAM untuk digunakan di Image Builder, lihat [AWS Identity and Access Management \(IAM\)](#) di Panduan Pengguna Image Builder.

Peran Anda membutuhkan:

- Hubungan tepercaya termasuk EC2 layanan Amazon.
- Amazon SSMManaged InstanceCore dan EC2 InstanceProfileForImageBuilder kebijakan.
- Kebijakan RES khusus dengan akses DynamoDB dan Amazon S3 terbatas ke lingkungan RES yang diterapkan.

(Kebijakan ini dapat berupa dokumen kebijakan inline yang dikelola pelanggan atau pelanggan.)

Entitas hubungan tepercaya:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Kebijakan RES:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RES DynamoDB Access",
      "Effect": "Allow",
      "Action": "dynamodb:GetItem",
      "Resource": "arn:aws:dynamodb:us-east-1:111122223333:table/{RES-EnvironmentName}.cluster-settings",
      "Condition": {
        "ForAllValues:StringLike": {
          "dynamodb:LeadingKeys": [
            "global-settings.gpu_settings.*",
            "global-settings.package_config.*",
            "cluster-manager.host_modules.*",
            "identity-provider.cognito.enable_native_user_login"
          ]
        }
      }
    },
    {
      "Sid": "RESS3Access",
```

```

        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": [
            "arn:aws:s3:::{RES-EnvironmentName}-cluster-us-east-1-111122223333/idea/vdc/res-ready-install-script-packages/*",
            "arn:aws:s3:::research-engineering-studio-us-east-1/host_modules/*"
        ]
    }
}

```

Buat komponen EC2 Image Builder

Ikuti petunjuk untuk [Membuat komponen menggunakan konsol Image Builder](#) di Panduan Pengguna Image Builder.

Masukkan detail komponen Anda:

1. Untuk Type, pilih Build.
2. Untuk sistem operasi Image (OS), pilih Linux atau Windows.
3. Untuk nama Komponen, masukkan nama yang bermakna seperti **research-and-engineering-studio-vdi-<operating-system>**.
4. Masukkan nomor versi komponen Anda dan tambahkan deskripsi secara opsional.
5. Untuk dokumen Definisi, masukkan file definisi berikut. Jika Anda menemukan kesalahan, file YAMM sensitif terhadap ruang dan merupakan penyebab yang paling mungkin.

Linux

```

# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the "License"). You may not
# use this file except in compliance
# with the License. A copy of the License is located at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# or in the 'license' file accompanying this file. This file is distributed on
# an 'AS IS' BASIS, WITHOUT WARRANTIES

```

```

# OR CONDITIONS OF ANY KIND, express or implied. See the License for the
# specific language governing permissions
# and limitations under the License.
name: research-and-engineering-studio-vdi-linux
description: An RES EC2 Image Builder component to install required RES software
dependencies for Linux VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
    type: string
    description: RES Environment AWS Account ID
  - RESEnvName:
    type: string
    description: RES Environment Name
  - RESEnvRegion:
    type: string
    description: RES Environment Region
  - RESEnvReleaseVersion:
    type: string
    description: RES Release Version

phases:
  - name: build
    steps:
      - name: PrepareRESBootstrap
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - 'mkdir -p /root/bootstrap/logs'
            - 'mkdir -p /root/bootstrap/latest'
      - name: DownloadRESLinuxInstallPackage
        action: S3Download
        onFailure: Abort
        maxAttempts: 3
        inputs:
          - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
            {{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
            res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
            destination: '/root/bootstrap/
            res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
            expectedBucketOwner: '{{ AWSAccountID }}'
      - name: RunInstallScript

```

```

        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
            commands:
                - 'tar -xvf
{{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
            - name: FirstReboot
              action: Reboot
              onFailure: Abort
              maxAttempts: 3
              inputs:
                delaySeconds: 0
            - name: RunInstallPostRebootScript
              action: ExecuteBash
              onFailure: Abort
              maxAttempts: 3
              inputs:
                commands:
                    - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
            - name: SecondReboot
              action: Reboot
              onFailure: Abort
              maxAttempts: 3
              inputs:
                delaySeconds: 0

```

Windows

```

# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the "License"). You may not
# use this file except in compliance
# with the License. A copy of the License is located at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# or in the 'license' file accompanying this file. This file is distributed on
# an 'AS IS' BASIS, WITHOUT WARRANTIES

```

```

# OR CONDITIONS OF ANY KIND, express or implied. See the License for the
# specific language governing permissions
# and limitations under the License.
name: research-and-engineering-studio-vdi-windows
description: An RES EC2 Image Builder component to install required RES software
dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
    type: string
    description: RES Environment AWS Account ID
  - RESEnvName:
    type: string
    description: RES Environment Name
  - RESEnvRegion:
    type: string
    description: RES Environment Region
  - RESEnvReleaseVersion:
    type: string
    description: RES Release Version

phases:
  - name: build
    steps:
      - name: CreateRESBootstrapFolder
        action: CreateFolder
        onFailure: Abort
        maxAttempts: 3
        inputs:
          - path: 'C:\Users\Administrator\RES\Bootstrap'
            overwrite: true
      - name: DownloadRESWindowsInstallPackage
        action: S3Download
        onFailure: Abort
        maxAttempts: 3
        inputs:
          - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
            {{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
            res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
            destination:
              '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
            expectedBucketOwner: '{{ AWSAccountID }}'
      - name: RunInstallScript
        action: ExecutePowerShell

```

```

    onFailure: Abort
    maxAttempts: 3
    inputs:
      commands:
        - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
        - 'Tar -xf
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
        - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
        - 'Install-WindowsEC2Instance'
  - name: Reboot
    action: Reboot
    onFailure: Abort
    maxAttempts: 3
    inputs:
      delaySeconds: 0

```

6. Buat tag opsional apa pun dan pilih Buat komponen.

Siapkan resep EC2 Image Builder Anda

Resep EC2 Image Builder mendefinisikan gambar dasar yang akan digunakan sebagai titik awal Anda untuk membuat gambar baru, bersama dengan kumpulan komponen yang Anda tambahkan untuk menyesuaikan gambar Anda dan memverifikasi bahwa semuanya berfungsi seperti yang diharapkan. Anda harus membuat atau memodifikasi resep untuk membangun AMI target dengan dependensi perangkat lunak RES yang diperlukan. Untuk informasi selengkapnya tentang resep, lihat [Mengelola resep](#).

RES mendukung sistem operasi gambar berikut:

- Amazon Linux 2 (x86 dan ARM64)
- Ubuntu 22.04.3 (x86)
- RHEL 8 (x86), dan 9 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Buka konsol EC2 Image Builder di <https://console.aws.amazon.com/imagebuilder>.
2. Di bawah Sumber daya tersimpan, pilih Resep gambar.
3. Pilih Buat resep gambar.

4. Masukkan nama unik dan nomor versi.
5. Pilih gambar dasar yang didukung oleh RES.
6. Di bawah konfigurasi Instans, instal agen SSM jika tidak diinstal sebelumnya. Masukkan informasi dalam data Pengguna dan data pengguna lain yang diperlukan.

 Note

Untuk informasi tentang cara menginstal agen SSM, lihat:

- [Menginstal Agen SSM secara manual pada EC2 instance untuk Linux.](#)
- [Menginstal dan menghapus instalasi Agen SSM secara manual pada EC2 instance untuk Windows Server.](#)

7. Untuk resep berbasis Linux, tambahkan komponen `aws-cli-version-2-linux` build yang dikelola Amazon ke resep. Skrip instalasi RES menggunakan AWS CLI untuk menyediakan akses VDI ke nilai konfigurasi untuk pengaturan cluster DynamoDB. Windows tidak memerlukan komponen ini.
8. Tambahkan komponen EC2 Image Builder yang dibuat untuk lingkungan Linux atau Windows Anda dan masukkan nilai parameter yang diperlukan. Parameter berikut adalah input yang diperlukan: AWSAccount ID, RESEnv Nama, RESEnv Wilayah, dan RESEnvReleaseVersion.

 Important

Untuk lingkungan Linux, Anda harus menambahkan komponen-komponen ini secara berurutan dengan komponen `aws-cli-version-2-linux` build yang ditambahkan terlebih dahulu.

9. (Disarankan) Tambahkan komponen `simple-boot-test-<linux-or-windows>` pengujian yang dikelola Amazon untuk memverifikasi bahwa AMI dapat diluncurkan. Ini adalah rekomendasi minimum. Anda dapat memilih komponen pengujian lain yang memenuhi kebutuhan Anda.
10. Lengkapi bagian opsional apa pun jika diperlukan, tambahkan komponen lain yang diinginkan, dan pilih Buat resep.

Modify a recipe

Jika Anda memiliki resep EC2 Image Builder yang sudah ada, Anda dapat menggunakannya dengan menambahkan komponen berikut:

1. Untuk resep berbasis Linux, tambahkan komponen `aws-cli-version-2-linux` build yang dikelola Amazon ke resep. Skrip instalasi RES menggunakan AWS CLI untuk menyediakan akses VDI ke nilai konfigurasi untuk pengaturan cluster DynamoDB. Windows tidak memerlukan komponen ini.
2. Tambahkan komponen EC2 Image Builder yang dibuat untuk lingkungan Linux atau Windows Anda dan masukkan nilai parameter yang diperlukan. Parameter berikut adalah input yang diperlukan: AWSAccount ID, RESEnv Nama, RESEnv Wilayah, dan RESEnvReleaseVersion.

Important

Untuk lingkungan Linux, Anda harus menambahkan komponen-komponen ini secara berurutan dengan komponen `aws-cli-version-2-linux` build yang ditambahkan terlebih dahulu.

3. Lengkapi bagian opsional apa pun jika diperlukan, tambahkan komponen lain yang diinginkan, dan pilih Buat resep.

Konfigurasikan infrastruktur EC2 Image Builder

Anda dapat menggunakan konfigurasi infrastruktur untuk menentukan EC2 infrastruktur Amazon yang digunakan Image Builder untuk membangun dan menguji image Image Builder Anda. Untuk digunakan dengan RES, Anda dapat memilih untuk membuat konfigurasi infrastruktur baru, atau menggunakan yang sudah ada.

- Untuk membuat konfigurasi infrastruktur baru, lihat [Membuat konfigurasi infrastruktur](#).
- Untuk menggunakan konfigurasi infrastruktur yang ada, [Perbarui konfigurasi infrastruktur](#).

Untuk mengonfigurasi infrastruktur Image Builder Anda:

1. Untuk peran IAM, masukkan peran yang telah Anda konfigurasikan sebelumnya. [Siapkan peran IAM untuk mengakses lingkungan RES](#)

2. Untuk tipe Instance, pilih tipe dengan memori minimal 4 GB dan dukung arsitektur AMI dasar pilihan Anda. Lihat [jenis EC2 Instans Amazon](#).
3. Untuk VPC, subnet, dan grup keamanan, Anda harus mengizinkan akses internet untuk mengunduh paket perangkat lunak. Akses juga harus diizinkan ke tabel `cluster-settings` DynamoDB dan bucket cluster Amazon S3 dari lingkungan RES.

Konfigurasi gambar Image Builder

Pipeline image Builder Image Builder merakit image dasar, komponen untuk pembuatan dan pengujian, konfigurasi infrastruktur, dan pengaturan distribusi. Untuk mengonfigurasi pipeline gambar untuk RES-ready AMIs, Anda dapat memilih untuk membuat pipeline baru, atau menggunakan pipeline yang sudah ada. Untuk informasi selengkapnya, lihat [Membuat dan memperbarui pipeline gambar AMI](#) di Panduan Pengguna Image Builder.

Create a new Image Builder pipeline

1. Buka konsol Image Builder di <https://console.aws.amazon.com/imagebuilder>.
2. Dari panel navigasi, pilih Pipeline gambar.
3. Pilih Buat pipeline gambar.
4. Tentukan detail pipeline Anda dengan memasukkan nama unik, deskripsi opsional, jadwal, dan frekuensi.
5. Untuk Pilih resep, pilih Gunakan resep yang ada dan pilih resep yang dibuat di [Siapkan resep EC2 Image Builder Anda](#). Verifikasi bahwa detail resep Anda benar.
6. Untuk proses pembuatan gambar, pilih alur kerja default atau kustom tergantung pada kasus penggunaan. Dalam kebanyakan kasus, alur kerja default sudah cukup. Untuk informasi selengkapnya, lihat [Mengonfigurasi alur kerja gambar untuk pipeline EC2 Image Builder](#).
7. Untuk Tentukan konfigurasi infrastruktur, pilih Pilih konfigurasi infrastruktur yang ada dan pilih konfigurasi infrastruktur yang dibuat [Konfigurasi infrastruktur EC2 Image Builder](#). Verifikasi bahwa detail infrastruktur Anda sudah benar.
8. Untuk Tentukan setelan distribusi, pilih Buat setelan distribusi menggunakan default layanan. Gambar output harus berada sama dengan lingkungan Wilayah AWS RES Anda. Menggunakan default layanan, gambar akan dibuat di Wilayah tempat Image Builder digunakan.
9. Tinjau detail pipeline dan pilih Create pipeline.

Modify an existing Image Builder pipeline

1. Untuk menggunakan pipeline yang ada, ubah detail untuk menggunakan resep yang dibuat [Siapkan resep EC2 Image Builder Anda](#).
2. Pilih Simpan perubahan.

Jalankan pipa gambar Image Builder

Untuk menghasilkan gambar keluaran yang dikonfigurasi, Anda harus memulai pipeline gambar. Proses pembangunan berpotensi memakan waktu hingga satu jam tergantung pada jumlah komponen dalam resep gambar.

Untuk menjalankan pipeline gambar:

1. Dari pipeline Image, pilih pipeline yang dibuat di [Konfigurasi pipa gambar Image Builder](#).
2. Dari Tindakan, pilih Jalankan pipeline.

Daftarkan tumpukan perangkat lunak baru di RES

1. Ikuti petunjuk [the section called “Tumpukan Perangkat Lunak \(\) AMIs”](#) untuk mendaftarkan tumpukan perangkat lunak.
2. Untuk ID AMI, masukkan ID AMI dari gambar keluaran bawaan [Jalankan pipa gambar Image Builder](#).

Panduan administrator

Panduan administrator ini memberikan instruksi tambahan untuk audiens teknis tentang cara menyesuaikan dan mengintegrasikan lebih lanjut dengan Studio Penelitian dan Teknik pada AWS produk.

Topik

- [Manajemen rahasia](#)
- [Pemantauan dan pengendalian biaya](#)
- [Manajemen sesi](#)
- [Pengelolaan lingkungan](#)

Manajemen rahasia

Research and Engineering Studio menyimpan rahasia berikut menggunakan AWS Secrets Manager. RES menciptakan rahasia secara otomatis selama pembuatan lingkungan. Rahasia yang dimasukkan oleh administrator selama pembuatan lingkungan dimasukkan sebagai parameter.

Nama rahasia	Deskripsi	RES dihasilkan	Admin masuk
<code><envname> -sso-client-secret</code>	Rahasia OAuth2 Klien Masuk Tunggal untuk lingkungan	✓	
<code><envname> -vdc-client-secret</code>	vdc ClientSecret	✓	
<code><envname> -vdc-client-id</code>	vdc ClientId	✓	
<code><envname> -vdc-gateway-certificate-private-key</code>	Kunci pribadi sertifikat yang ditandatangani sendiri untuk domain	✓	

Nama rahasia	Deskripsi	RES dihasilkan	Admin masuk
<code><envname> - vdc-gateway-certificate-certificate</code>	Sertifikat Self-Signed untuk domain	✓	
<code><envname> -cluster-manager-client-secret</code>	pengelola klaster ClientSecret	✓	
<code><envname> -cluster-manager-client-id</code>	pengelola klaster ClientId	✓	
<code><envname> -external-private-key</code>	Kunci pribadi sertifikat yang ditandatangani sendiri untuk domain	✓	
<code><envname> -external-certificate</code>	Sertifikat Self-Signed untuk domain	✓	
<code><envname> -internal-private-key</code>	Kunci pribadi sertifikat yang ditandatangani sendiri untuk domain	✓	
<code><envname> -internal-certificate</code>	Sertifikat Self-Signed untuk domain	✓	
<code><envname> -director-service-ServiceAccountUserDN</code>	Atribut Distinguished Name (DN) dari ServiceAccount pengguna.	✓	

Nilai ARN rahasia berikut terkandung dalam *<envname>*-cluster-settings tabel di DynamoDB:

Kunci	Sumber
<code>identity-provider.cognito.sso_client_secret</code>	
<code>vdc.dcv_connection_gateway.certificate.certificate_secret_arn</code>	tumpukan
<code>vdc.dcv_connection_gateway.certificate.private_key_secret_arn</code>	tumpukan
<code>cluster.load_balancers.internal_alb.certificates.private_key_secret_arn</code>	tumpukan
<code>directoryservice.root_username_secret_arn</code>	
<code>vdc.client_secret</code>	tumpukan
<code>cluster.load_balancers.external_alb.certificates.certificate_secret_arn</code>	tumpukan
<code>cluster.load_balancers.internal_alb.certificates.certificate_secret_arn</code>	tumpukan
<code>directoryservice.root_password_secret_arn</code>	
<code>cluster.secretsmanager.kms_key_id</code>	
<code>cluster.load_balancers.external_alb.certificates.private_key_secret_arn</code>	tumpukan
<code>cluster-manager.client_secret</code>	

Pemantauan dan pengendalian biaya

Note

Mengaitkan proyek Studio Penelitian dan Teknik ke AWS Budgets tidak didukung di AWS GovCloud (US).

Sebaiknya buat [anggaran](#) melalui [AWS Cost Explorer](#) untuk membantu mengelola biaya. Harga dapat berubah sewaktu-waktu. Untuk detail selengkapnya, lihat halaman web harga untuk masing-masing. [the section called “AWS layanan dalam produk ini”](#)

Untuk membantu pelacakan biaya, Anda dapat mengaitkan proyek RES dengan anggaran yang dibuat di dalamnya AWS Budgets. Pertama-tama Anda harus mengaktifkan tag lingkungan dalam tag alokasi biaya penagihan.

1. Masuk ke AWS Management Console dan buka AWS Manajemen Penagihan dan Biaya konsol di <https://console.aws.amazon.com/costmanagement/>.
2. Pilih Tag alokasi biaya.
3. Cari dan pilih `res:Project` dan `res:EnvironmentName` tag.
4. Pilih Aktifkan.

Note

Mungkin diperlukan waktu hingga satu hari agar tag RES muncul setelah penerapan.

Untuk membuat anggaran untuk sumber daya RES:

1. Dari konsol Penagihan, pilih Anggaran.
2. Pilih Buat anggaran.
3. Di bawah Pengaturan anggaran, pilih Sesuaikan (lanjutan).
4. Di bawah Jenis anggaran, pilih Anggaran biaya - Direkomendasikan.
5. Pilih Berikutnya.

6. Di bawah Detail, masukkan nama Anggaran yang berarti untuk anggaran Anda untuk membedakannya dari anggaran lain di akun Anda. Misalnya, *<EnvironmentName>-<ProjectName>-<BudgetName>*.
7. Di bawah Tetapkan jumlah anggaran, masukkan jumlah yang dianggarkan untuk proyek Anda.
8. Di bawah cakupan Anggaran, pilih Filter dimensi AWS biaya tertentu.
9. Pilih Tambahkan filter.
10. Di bawah Dimensi, pilih Tag.
11. Di bawah Tag, pilih RES:Project.

 Note

Mungkin diperlukan waktu hingga dua hari agar tag dan nilai tersedia. Anda dapat membuat anggaran setelah nama proyek tersedia.

12. Di bawah Nilai, pilih nama proyek.
13. Pilih Terapkan filter untuk melampirkan filter proyek ke anggaran.
14. Pilih Berikutnya.
15. (Opsional.) Tambahkan ambang peringatan.
16. Pilih Berikutnya.
17. (Opsional.) Jika peringatan telah dikonfigurasi, gunakan Lampirkan tindakan untuk mengonfigurasi tindakan yang diinginkan dengan peringatan.
18. Pilih Berikutnya.
19. Tinjau konfigurasi anggaran dan konfirmasi tag yang benar telah ditetapkan di bawah Parameter anggaran tambahan.
20. Pilih Buat anggaran.

Sekarang anggaran telah dibuat, Anda dapat mengaktifkan anggaran untuk proyek. Untuk mengaktifkan anggaran untuk suatu proyek, lihat [the section called “Mengedit proyek”](#). Desktop virtual akan diblokir dari peluncuran jika anggaran terlampaui. Jika anggaran terlampaui saat desktop diluncurkan, desktop akan terus beroperasi.

Jika Anda perlu mengubah anggaran Anda, kembali ke konsol untuk mengedit jumlah anggaran. Mungkin diperlukan waktu hingga lima belas menit agar perubahan diterapkan dalam RES. Atau, Anda dapat mengedit proyek untuk menonaktifkan anggaran.

Manajemen sesi

Manajemen sesi menyediakan lingkungan yang fleksibel dan interaktif untuk mengembangkan dan menguji sesi. Sebagai pengguna administratif, Anda dapat mengizinkan pengguna untuk membuat dan mengelola sesi interaktif dalam lingkungan proyek mereka.

Topik

- [Dasbor](#)
- [Sesi](#)
- [Tumpukan Perangkat Lunak \(\) AMLs](#)
- [Debugging](#)
- [Pengaturan desktop](#)

Dasbor

Dasbor Manajemen Sesi menyediakan administrator dengan pandangan cepat ke:

1. Tipe instans
2. Sesi menyatakan
3. OS dasar
4. Proyek
5. Zona ketersediaan
6. Tumpukan perangkat lunak

Selain itu, administrator dapat:

7. Segarkan dasbor untuk memperbarui informasi.
8. Pilih Lihat Sesi untuk menavigasi ke Sesi.

Sesi

Sesi menampilkan semua desktop virtual yang dibuat dalam Research and Engineering Studio. Dari halaman Sesi, Anda dapat memfilter dan melihat informasi sesi atau membuat sesi baru.

1. Gunakan menu untuk memfilter hasil berdasarkan sesi yang dibuat atau diperbarui dalam jangka waktu tertentu.
2. Pilih sesi dan gunakan menu Tindakan untuk:
 - a. Sesi Lanjutkan
 - b. Stop/Hibernate Sesi
 - c. Stop/Hibernate Sesi Paksa
 - d. Mengakhiri Sesi
 - e. Paksa Mengakhiri Sesi
 - f. Sesi Kesehatan
 - g. Buat Tumpukan Perangkat Lunak
3. Pilih Buat Sesi untuk membuat sesi baru.
4. Cari sesi berdasarkan nama dan filter menurut status dan sistem operasi.
5. Pilih Nama Sesi untuk melihat detail selengkapnya.

Buat sesi

1. Pilih Buat Sesi. Modal Launch New Virtual Desktop terbuka.
2. Masukkan detail untuk sesi baru.
3. (Opsional.) Aktifkan Tampilkan Opsi Lanjutan untuk memberikan detail tambahan seperti subnet ID dan jenis sesi DCV.
4. Pilih Kirim.

Rincian sesi

Dari daftar Sesi, pilih Nama Sesi untuk melihat detail sesi.

Tumpukan Perangkat Lunak () AMIs

Note

Untuk menjalankan tumpukan SO7 perangkat lunak Cent yang disediakan AWS GovCloud (US), Anda harus berlangganan AMI dalam AWS Marketplace menggunakan [akun standar tertaut](#) Anda.

Dari halaman Tumpukan Perangkat Lunak, Anda dapat mengonfigurasi Amazon Machine Images (AMIs) atau mengelola yang sudah ada.

1. Untuk mencari tumpukan perangkat lunak yang ada, gunakan drop-down sistem operasi untuk memfilter berdasarkan OS.
2. Pilih nama tumpukan perangkat lunak untuk melihat detail tentang tumpukan.
3. Setelah Anda memilih tumpukan perangkat lunak, gunakan menu Tindakan untuk mengedit tumpukan dan menetapkan tumpukan ke proyek.
4. Tombol Register Software Stack memungkinkan Anda membuat tumpukan baru:
 1. Pilih Daftarkan Tumpukan Perangkat Lunak.
 2. Masukkan detail untuk tumpukan perangkat lunak baru.
 3. Pilih Kirim.

Tetapkan tumpukan perangkat lunak ke proyek

Saat Anda membuat tumpukan perangkat lunak baru, Anda dapat menetapkan tumpukan ke proyek. Jika Anda perlu menambahkan tumpukan ke proyek setelah pembuatan awal, lakukan hal berikut:

Note

Anda hanya dapat menetapkan tumpukan perangkat lunak ke proyek di mana Anda menjadi anggotanya.

1. Pilih tumpukan perangkat lunak yang perlu Anda tambahkan ke proyek dari halaman Software Stacks.
2. Pilih Tindakan.
3. Pilih Edit.
4. Gunakan drop-down Proyek untuk memilih proyek.
5. Pilih Kirim.

Anda juga dapat mengedit tumpukan perangkat lunak dari halaman detail tumpukan.

Lihat detail tumpukan perangkat lunak

Dari daftar Tumpukan Perangkat Lunak, pilih Nama Tumpukan Perangkat Lunak untuk melihat detailnya. Dari halaman detail, Anda juga dapat memilih Edit untuk mengedit tumpukan perangkat lunak.

Debugging

Panel debugging menampilkan lalu lintas pesan yang terkait dengan desktop virtual. Anda dapat menggunakan panel ini untuk mengamati aktivitas antar host. Tab Host VD menampilkan aktivitas spesifik instance, dan tab Sesi VD menampilkan aktivitas sesi yang sedang berlangsung.

Pengaturan desktop

Anda dapat menggunakan halaman Pengaturan Desktop untuk mengonfigurasi sumber daya yang terkait dengan desktop virtual. Tab Server menyediakan akses ke pengaturan seperti:

Batas waktu idle sesi DCV

Waktu setelah sesi DCV akan terputus secara otomatis. Ini tidak mengubah keadaan sesi desktop, itu hanya menutup sesi dari klien DCV atau browser web.

Peringatan batas waktu idle

Waktu setelah itu peringatan mengganggu akan diberikan kepada klien.

Ambang batas pemanfaatan CPU

Pemanfaatan CPU dianggap idle.

Sesi yang diizinkan per pengguna

Jumlah sesi VDI yang dapat dimiliki pengguna individu pada waktu tertentu. Jika pengguna memenuhi atau melampaui nilai ini, ini akan mencegah mereka meluncurkan sesi baru dari halaman Desktop Virtual Saya. Kemampuan untuk meluncurkan sesi melalui halaman Sessions tidak terpengaruh oleh nilai ini.

Ukuran volume akar maks

Ukuran default volume root pada sesi desktop virtual.

Jenis contoh yang diizinkan

Daftar keluarga dan ukuran instance yang dapat diluncurkan untuk lingkungan RES ini. Keluarga instance dan kombinasi ukuran instance keduanya diterima. Misalnya, jika Anda menentukan 'm7a', semua ukuran keluarga m7a akan tersedia untuk diluncurkan sebagai sesi VDI. Jika Anda menentukan 'm7a.24xlarge', hanya m7a.24xlarge yang akan tersedia untuk diluncurkan sebagai sesi VDI. Daftar ini memengaruhi semua proyek di lingkungan.

Pengelolaan lingkungan

Dari bagian manajemen Lingkungan Studio Riset dan Teknik, pengguna administratif dapat membuat dan mengelola lingkungan yang terisolasi untuk proyek penelitian dan rekayasa mereka. Lingkungan ini dapat mencakup sumber daya komputasi, penyimpanan, dan komponen lain yang diperlukan, semuanya dalam lingkungan yang aman. Pengguna dapat mengonfigurasi dan menyesuaikan lingkungan ini untuk memenuhi persyaratan spesifik proyek mereka, sehingga lebih mudah untuk bereksperimen, menguji, dan mengulangi solusi mereka tanpa memengaruhi proyek atau lingkungan lain.

Topik

- [Status lingkungan](#)
- [Pengaturan lingkungan](#)
- [Pengguna](#)
- [Grup](#)
- [Proyek](#)
- [Kebijakan izin](#)

- [Sistem File](#)
- [Manajemen snapshot](#)
- [Bucket Amazon S3](#)

Status lingkungan

Halaman Status Lingkungan menampilkan perangkat lunak dan host yang digunakan dalam produk. Ini mencakup informasi seperti versi perangkat lunak, nama modul, dan informasi sistem lainnya.

Pengaturan lingkungan

Halaman pengaturan Lingkungan menampilkan detail konfigurasi produk, seperti:

- Umum

Menampilkan informasi seperti Nama Pengguna Administrator dan email untuk pengguna yang menyediakan produk. Anda dapat mengedit judul portal web dan teks hak cipta.

- Penyedia Identitas

Menampilkan informasi seperti status Single Sign-On.

- Jaringan

Menampilkan ID VPC, daftar IDs Awal untuk akses.

- Directory Service

Menampilkan pengaturan direktori aktif dan manajer rahasia akun layanan ARN untuk nama pengguna dan kata sandi.

Pengguna

Semua pengguna yang disinkronkan dari direktori aktif Anda akan muncul di halaman Pengguna. Pengguna disinkronkan oleh pengguna cluster-admin selama konfigurasi produk. Untuk informasi selengkapnya tentang konfigurasi pengguna awal, lihat [Panduan konfigurasi](#).

 Note

Administrator hanya dapat membuat sesi untuk pengguna aktif. Secara default, semua pengguna akan berada dalam keadaan tidak aktif hingga mereka masuk ke lingkungan produk. Jika pengguna tidak aktif, minta mereka untuk masuk sebelum membuat sesi untuk mereka.

Dari halaman Pengguna, Anda dapat:

1. Cari pengguna.
2. Saat nama pengguna dipilih, gunakan menu Tindakan untuk:
 - a. Tetapkan sebagai pengguna Admin
 - b. Nonaktifkan pengguna

Grup

Semua Grup yang disinkronkan dari direktori aktif muncul di halaman Grup. Untuk informasi selengkapnya tentang konfigurasi dan manajemen grup, lihat [Panduan konfigurasi](#).

Dari halaman Grup, Anda dapat:

1. Cari grup pengguna.
2. Saat grup pengguna dipilih, gunakan menu Tindakan untuk menonaktifkan atau mengaktifkan grup.
3. Saat grup pengguna dipilih, Anda dapat memperluas panel Pengguna di bagian bawah layar untuk melihat pengguna dalam grup.

Proyek

Proyek membentuk batas untuk desktop virtual, tim, dan anggaran. Saat Anda membuat proyek, Anda menentukan pengaturannya, seperti nama, deskripsi, dan konfigurasi lingkungan. Proyek biasanya mencakup satu atau lebih lingkungan, yang dapat disesuaikan untuk memenuhi

persyaratan spesifik proyek Anda, seperti jenis dan ukuran sumber daya komputasi, tumpukan perangkat lunak, dan konfigurasi jaringan.

Topik

- [Lihat proyek](#)
- [Membuat proyek](#)
- [Mengedit proyek](#)
- [Menambahkan atau menghapus tag dari proyek](#)
- [Lihat sistem file yang terkait dengan proyek](#)
- [Tambahkan template peluncuran](#)

Lihat proyek

Dasbor Proyek menyediakan daftar proyek yang tersedia untuk Anda. Dari dasbor Proyek, Anda dapat:

1. Anda dapat menggunakan bidang pencarian untuk menemukan proyek.
2. Saat proyek dipilih, Anda dapat menggunakan menu Tindakan untuk:
 - a. Mengedit proyek
 - b. Nonaktifkan atau aktifkan proyek
 - c. Perbarui tag proyek
3. Anda dapat memilih Create Project untuk membuat proyek baru.

Membuat proyek

1. Pilih Buat Proyek.
2. Masukkan detail proyek.

Project ID adalah tag sumber daya yang dapat digunakan untuk melacak alokasi biaya. AWS Cost Explorer Service Untuk informasi selengkapnya, lihat [Mengaktifkan tag alokasi biaya yang ditentukan pengguna](#).

 Important

ID proyek tidak dapat diubah setelah pembuatan.

Untuk informasi tentang Opsi Lanjutan, lihat [Tambahkan template peluncuran](#).

3. (Opsional) Aktifkan anggaran untuk proyek. Untuk informasi lebih lanjut tentang anggaran, lihat [Pemantauan dan pengendalian biaya](#).
4. Sistem file direktori home dapat menggunakan Shared Home Filesystem (default), EFS, FSx untuk penyimpanan volume Lustre, ONTAP, atau EBS. FSx NetApp

Penting untuk dicatat bahwa sistem file rumah bersama, EFS, FSx untuk Lustre, dan FSx NetApp ONTAP dapat dibagikan di beberapa proyek dan VDI. Namun, opsi penyimpanan volume EBS akan mengharuskan setiap VDI dalam proyek itu untuk memiliki direktori home mereka sendiri yang tidak dibagi antara proyek lain VDI atau proyek.

5. Tetapkan and/or grup pengguna peran yang sesuai (“Anggota Proyek” atau “Pemilik Proyek”). Lihat [Profil izin default](#) tindakan yang dapat diambil setiap peran.
6. Pilih Kirim.

Mengedit proyek

1. Pilih proyek dalam daftar proyek.
2. Dari menu Tindakan, pilih Edit Proyek.
3. Masukkan pembaruan Anda.

Jika Anda ingin mengaktifkan anggaran, lihat [Pemantauan dan pengendalian biaya](#) untuk informasi selengkapnya. Ketika Anda memilih anggaran untuk proyek, mungkin ada penundaan beberapa detik untuk opsi dropdown anggaran untuk dimuat— jika Anda tidak melihat anggaran yang baru saja Anda buat, pilih tombol segarkan di sebelah dropdown.

Untuk informasi tentang Opsi Lanjutan, lihat [Tambahkan template peluncuran](#).

4. Pilih Kirim.

Menambahkan atau menghapus tag dari proyek

Tag proyek akan menetapkan tag ke semua instance yang dibuat di bawah proyek itu.

1. Pilih proyek dalam daftar proyek.
2. Dari menu Tindakan, pilih Perbarui Tag.
3. Pilih Tambahkan Tag dan masukkan nilai untuk Kunci.
4. Untuk menghapus tag, pilih Hapus di samping tag yang ingin Anda hapus.

Lihat sistem file yang terkait dengan proyek

Ketika proyek dipilih, Anda dapat memperluas panel Sistem File di bagian bawah layar untuk melihat sistem file yang terkait dengan proyek.

Tambahkan template peluncuran

Saat membuat atau mengedit proyek, Anda dapat menambahkan templat peluncuran menggunakan Opsi Lanjutan dalam konfigurasi proyek. Template peluncuran menyediakan konfigurasi tambahan, seperti grup keamanan, kebijakan IAM, dan skrip peluncuran ke semua instance VDI dalam proyek.

Tambahkan kebijakan

Anda dapat menambahkan kebijakan IAM untuk mengontrol akses VDI untuk semua instance yang diterapkan di proyek Anda. Untuk melakukan onboard kebijakan, beri tag kebijakan dengan pasangan nilai kunci berikut:

```
res:Resource/vdi-host-policy
```

Untuk informasi selengkapnya tentang peran IAM, lihat [Kebijakan dan izin di IAM](#).

Tambahkan grup keamanan

Anda dapat menambahkan grup keamanan untuk mengontrol data keluar dan masuk untuk semua instans VDI di bawah proyek Anda. Untuk onboard grup keamanan, beri tag grup keamanan dengan pasangan kunci-nilai berikut:

```
res:Resource/vdi-security-group
```

Untuk informasi selengkapnya tentang grup keamanan, lihat [Mengontrol lalu lintas ke AWS sumber daya Anda menggunakan grup keamanan](#) di Panduan Pengguna Amazon VPC.

Tambahkan skrip peluncuran

Anda dapat menambahkan skrip peluncuran yang akan dimulai pada semua sesi VDI dalam proyek Anda. RES mendukung inisiasi skrip untuk Linux dan Windows. Untuk inisiasi skrip, Anda dapat memilih:

Jalankan Script Saat VDI Dimulai

Opsi ini memulai skrip di awal instance VDI sebelum konfigurasi atau instalasi RES dijalankan.

Jalankan Script saat VDI Dikonfigurasi

Opsi ini memulai skrip setelah konfigurasi RES selesai.

Skrip mendukung opsi berikut:

Konfigurasi skrip	Contoh
URI S3	s3://bucketname/script.sh
URL HTTPS	https://sample.samplecontent.com/sampel
Berkas lokal	berkas:///sh user/scripts/example

Untuk Argumen, berikan argumen apa pun yang dipisahkan dengan koma.

Contoh konfigurasi proyek

Kebijakan izin

Research and Engineering Studio (RES) memungkinkan pengguna administratif untuk membuat profil izin khusus yang memberikan izin tambahan kepada pengguna terpilih untuk mengelola proyek yang menjadi bagiannya. Setiap proyek dilengkapi dengan dua [profil izin default](#) - “Anggota Proyek” dan “Pemilik Proyek” yang dapat disesuaikan setelah penerapan.

Saat ini, administrator dapat memberikan dua koleksi izin menggunakan profil izin:

1. Izin manajemen proyek yang terdiri dari “Perbarui keanggotaan proyek” yang memungkinkan pengguna yang ditunjuk untuk menambahkan pengguna dan grup lain ke, atau menghapusnya dari, proyek, dan “Perbarui status proyek” yang memungkinkan pengguna yang ditunjuk untuk mengaktifkan atau menonaktifkan proyek.
2. Izin manajemen sesi VDI yang terdiri dari “Buat Sesi” yang memungkinkan pengguna yang ditunjuk untuk membuat sesi VDI dalam proyek mereka, dan “Buat/Hentikan sesi pengguna lain” yang memungkinkan pengguna yang ditunjuk untuk membuat atau mengakhiri sesi pengguna lain dalam sebuah proyek.

Dengan cara ini, administrator dapat mendelegasikan izin berbasis proyek ke non-administrator di lingkungan mereka.

Topik

- [Izin manajemen proyek](#)
- [Izin manajemen sesi VDI](#)
- [Mengelola profil izin](#)
- [Profil izin default](#)
- [Batas lingkungan](#)
- [Profil berbagi desktop](#)

Izin manajemen proyek

Perbarui keanggotaan proyek

Izin ini memungkinkan pengguna non-admin yang telah diberikan untuk menambah dan menghapus pengguna atau grup dari proyek. Ini juga memungkinkan mereka untuk mengatur profil izin dan memutuskan tingkat akses untuk semua pengguna dan grup lain untuk proyek itu.

Perbarui status proyek

Izin ini memungkinkan pengguna non-admin yang telah diberikan untuk mengaktifkan atau menonaktifkan proyek menggunakan tombol Tindakan pada halaman Proyek.

Izin manajemen sesi VDI

Buat sesi

Mengontrol apakah pengguna diizinkan untuk meluncurkan sesi VDI mereka sendiri dari halaman Desktop Virtual Saya atau tidak. Nonaktifkan ini untuk menolak pengguna non-admin kemampuan untuk meluncurkan sesi VDI mereka sendiri. Pengguna selalu dapat menghentikan dan mengakhiri sesi VDI mereka sendiri.

Jika pengguna non-admin tidak memiliki izin untuk membuat sesi, tombol Luncurkan Desktop Virtual Baru akan dinonaktifkan untuk mereka seperti yang ditunjukkan di sini:

Membuat atau Mengakhiri sesi orang lain

Memungkinkan pengguna non-admin mengakses halaman Sesi dari panel navigasi sebelah kiri. Pengguna ini akan dapat meluncurkan sesi VDI untuk pengguna lain dalam proyek di mana mereka telah diberikan izin ini.

Jika pengguna non-admin memiliki izin untuk meluncurkan sesi untuk pengguna lain, panel navigasi sebelah kiri mereka akan menampilkan tautan Sesi di bawah Manajemen Sesi seperti yang ditunjukkan di sini:

Jika pengguna non-admin tidak memiliki izin untuk membuat sesi untuk orang lain, panel navigasi sebelah kiri mereka tidak akan menampilkan Manajemen Sesi seperti yang ditunjukkan di sini:

Mengelola profil izin

Sebagai administrator RES, Anda dapat melakukan tindakan berikut untuk mengelola profil izin.

Daftar profil izin

- Dari halaman konsol Studio Penelitian dan Rekayasa, pilih Kebijakan izin di panel navigasi sebelah kiri. Dari halaman ini Anda dapat membuat, memperbarui, membuat daftar, melihat, dan menghapus profil izin.

Lihat profil izin

1. Pada halaman Profil Izin utama, pilih nama profil izin yang ingin Anda lihat. Dari halaman ini Anda dapat mengedit atau menghapus profil izin yang dipilih.
2. Pilih tab Proyek yang terpengaruh untuk melihat proyek yang saat ini menggunakan profil izin.

Buat profil izin

1. Pada halaman Profil Izin utama, pilih Buat profil untuk membuat profil izin.
2. Masukkan nama dan deskripsi profil izin, lalu pilih izin yang akan diberikan kepada pengguna atau grup yang Anda tetapkan ke profil ini.

Edit profil izin

- Pada halaman Profil Izin utama, pilih profil dengan mengklik lingkaran di sebelahnya, pilih Tindakan, lalu pilih Edit profil untuk memperbarui profil izin tersebut.

Hapus profil izin

- Pada halaman Profil Izin utama, pilih profil dengan mengklik lingkaran di sebelahnya, pilih Tindakan, lalu pilih Hapus profil. Anda tidak dapat menghapus profil izin yang digunakan oleh proyek yang ada.

Profil izin default

Setiap proyek RES dilengkapi dengan dua profil izin default yang dapat dikonfigurasi oleh Administrator Global. (Selain itu, Administrator Global dapat membuat dan memodifikasi profil izin baru untuk sebuah proyek.) Tabel berikut menunjukkan izin yang diizinkan untuk profil izin default-“Anggota Proyek” dan “Pemilik Proyek”. Profil izin, dan izin yang mereka berikan untuk memilih pengguna proyek, hanya berlaku untuk proyek milik mereka; Administrator Global adalah pengguna super yang memiliki semua izin di bawah ini di semua proyek.

Izin	Deskripsi	Anggota Proyek	Pemilik Proyek	
Buat Sesi	Buat sesi Anda sendiri. Pengguna selalu dapat menghentikan dan mengakhiri sesi mereka sendiri dengan atau tanpa izin ini.	X	X	
Buat/akhiri sesi orang lain	Membuat atau mengakhiri sesi pengguna lain dalam sebuah proyek.		X	
Perbarui keanggotaan Proyek	Perbarui pengguna dan grup yang terkait dengan proyek.		X	
Perbarui Status Proyek	Aktifkan atau nonaktifkan proyek.		X	

Batas lingkungan

Batas lingkungan memungkinkan administrator Research and Engineering Studio (RES) untuk mengonfigurasi izin yang akan berlaku secara global untuk semua pengguna. Ini termasuk izin seperti Peramban File dan izin SSH, Izin Desktop, dan pengaturan lanjutan Desktop.

Mengkonfigurasi akses browser File

Administrator RES dapat mengaktifkan atau menonaktifkan data Access di bawah izin browser File. Jika data Access dimatikan, pengguna tidak akan melihat navigasi File Browser di portal web mereka dan tidak dapat mengunggah atau mengunduh data yang dilampirkan ke sistem file global mereka. Ketika data Access diaktifkan, pengguna memiliki akses ke navigasi File Browser di portal web mereka yang memungkinkan mereka untuk mengunggah atau mengunduh data yang dilampirkan ke sistem file global mereka.

Ketika fitur Access data diaktifkan dan kemudian dimatikan, pengguna yang sudah masuk ke portal web tidak akan dapat mengunggah atau mengunduh file, bahkan jika mereka berada di halaman yang sesuai. Selain itu, menu navigasi akan hilang ketika mereka menyegarkan halaman.

Mengkonfigurasi akses SSH

Administrator dapat mengaktifkan atau menonaktifkan SSH untuk lingkungan RES dari bagian batas Lingkungan. Akses SSH ke VDIs difasilitasi melalui host benteng. Saat Anda mengaktifkan sakelar ini, RES menyebarkan host bastion dan membuat halaman Instruksi Akses SSH terlihat bagi pengguna. Saat Anda menonaktifkan sakelar, RES menonaktifkan akses SSH, menghentikan host bastion dan menghapus halaman instruksi akses SSH untuk pengguna. Toggle ini dinonaktifkan secara default.

Note

Saat RES menyebarkan host bastion, ia menambahkan EC2 instans t3.medium Amazon di akun Anda AWS. Anda bertanggung jawab atas semua biaya yang terkait dengan contoh ini. Lihat [halaman EC2 harga Amazon](#) untuk informasi lebih lanjut.

Untuk mengaktifkan akses SSH

1. Di konsol RES, di panel navigasi kiri, pilih Manajemen Lingkungan, lalu Kebijakan Izin. Di bawah batas Lingkungan pilih sakelar akses SSH.
2. Tunggu akses SSH diaktifkan.
3. Setelah host Bastion ditambahkan, akses SSH diaktifkan.

Halaman Petunjuk Akses SSH dapat dilihat oleh pengguna dari panel navigasi kiri mereka.

Untuk menonaktifkan akses SSH

1. Di konsol RES, di panel navigasi kiri, pilih Manajemen Lingkungan, lalu Kebijakan Izin. Di bawah batas Lingkungan pilih sakelar akses SSH.
2. Tunggu akses SSH dinonaktifkan.
3. Setelah proses selesai, akses SSH dinonaktifkan.

Mengkonfigurasi Izin Desktop

Administrator dapat mengaktifkan atau menonaktifkan izin Desktop untuk mengelola fungsionalitas VDI semua pemilik sesi secara global. Semua izin ini, atau subset, dapat digunakan untuk membuat profil berbagi Desktop yang menentukan tindakan mana yang dapat dilakukan oleh pengguna dengan siapa desktop dibagikan. Jika ada izin desktop yang dinonaktifkan, ini akan secara otomatis menonaktifkan izin yang sesuai di profil berbagi Desktop. Izin ini akan diberi label sebagai “Dinonaktifkan Secara Global”. Bahkan jika administrator mengaktifkan izin desktop ini lagi, izin di profil berbagi desktop akan tetap dinonaktifkan sampai administrator mengaktifkannya secara manual.

Profil berbagi desktop

Administrator dapat membuat profil baru dan menyesuaikannya. Profil ini dapat diakses oleh semua pengguna dan digunakan saat berbagi sesi dengan orang lain. Izin maksimum yang diberikan dalam profil ini tidak dapat melebihi izin desktop yang diizinkan secara global.

Buat Profil

Administrator dapat memilih Buat profil untuk membuat profil baru. Kemudian mereka dapat memasukkan nama Profil, Deskripsi Profil, mengatur izin yang diinginkan, dan Simpan perubahan mereka.

Edit Profil

Untuk mengedit profil:

1. Pilih profil yang diinginkan.
2. Pilih Tindakan, lalu pilih Edit untuk mengubah profil.
3. Sesuaikan izin sesuai kebutuhan.
4. Pilih Simpan perubahan.

Setiap perubahan yang dilakukan pada profil akan segera diterapkan ke sesi terbuka saat ini.

Sistem File

Dari halaman File Systems, Anda dapat:

1. Cari sistem file.
2. Saat sistem file dipilih, gunakan menu Tindakan untuk:
 - a. Tambahkan sistem file ke proyek.
 - b. Hapus sistem file dari proyek
3. Onboard sistem file baru.
4. Saat sistem file dipilih, Anda dapat memperluas panel di bagian bawah layar untuk melihat detail sistem file.

Topik

- [Onboard sistem file](#)

Onboard sistem file

1. Pilih Sistem File Onboard.

2. Pilih sistem file dari drop down. Modal akan berkembang dengan entri detail tambahan.
3. Masukkan detail sistem file.

 Note

Secara default, administrator dan pemilik proyek memiliki kemampuan untuk memilih sistem file rumah saat membuat proyek baru, yang tidak dapat diedit setelahnya. Sistem file yang dimaksudkan untuk digunakan sebagai direktori home pada proyek harus di-onboard dengan menyetel jalur Mount Directory ke. /home Ini akan mengisi sistem file onboard pada opsi dropdown sistem file direktori home. Fitur ini membantu menjaga data terisolasi di seluruh proyek karena hanya pengguna yang terkait dengan proyek yang akan memiliki akses ke sistem file melalui mereka. VDI akan memasang sistem file pada titik pemasangan yang dipilih selama orientasi sistem file.

4. Pilih Kirim.

Manajemen snapshot

Manajemen snapshot menyederhanakan proses penyimpanan dan migrasi data antar lingkungan, memastikan konsistensi dan akurasi. Dengan snapshot, Anda dapat menyimpan status lingkungan dan memigrasikan data ke lingkungan baru dengan status yang sama.

Dari halaman manajemen Snapshot, Anda dapat:

1. Lihat semua snapshot yang dibuat dan statusnya.
2. Buat snapshot. Sebelum Anda dapat membuat snapshot, Anda harus membuat ember dengan izin yang sesuai.
3. Lihat semua snapshot yang diterapkan dan statusnya.
4. Terapkan snapshot.

Topik

- [Buat snapshot](#)
- [Terapkan snapshot](#)

Buat snapshot

Sebelum Anda dapat membuat snapshot, Anda harus memberikan bucket Amazon S3 dengan izin yang diperlukan. Untuk informasi tentang membuat bucket, lihat [Membuat bucket](#). Sebaiknya aktifkan pembuatan versi bucket dan pencatatan akses server. Pengaturan ini dapat diaktifkan dari tab Properties bucket setelah penyediaan.

Note

Siklus hidup bucket Amazon S3 ini tidak akan dikelola dalam produk. Anda perlu mengelola siklus hidup bucket dari konsol.

Untuk menambahkan izin ke bucket:

1. Pilih bucket yang Anda buat dari daftar Bucket.
2. Pilih tab Izin.
3. Di Bawah Kebijakan bucket, pilih Edit.
4. Tambahkan pernyataan berikut ke kebijakan bucket. Ganti nilai-nilai ini dengan nilai Anda sendiri:
 - **111122223333**-> ID AWS Akun Anda
 - **{RES_ENVIRONMENT_NAME}**-> nama lingkungan RES Anda
 - **us-east-1**-> AWS wilayah Anda
 - **amzn-s3-demo-bucket**-> nama ember S3 Anda

Important

Ada string versi terbatas yang didukung oleh AWS. Untuk informasi selengkapnya, lihat https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "Export-Snapshot-Policy",
        "Effect": "Allow",
        "Principal": {
          "AWS":
            "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
            role-us-east-1}"
        },
        "Action": [
          "s3:GetObject",
          "s3:ListBucket",
          "s3:AbortMultipartUpload",
          "s3:PutObject",
          "s3:PutObjectAcl"
        ],
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket",
          "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
      },
      {
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket",
          "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
          "Bool": {
            "aws:SecureTransport": "false"
          }
        },
        "Principal": "*"
      }
    ]
  }
}

```

Untuk membuat snapshot:

1. Pilih Buat Snapshot.

2. Masukkan nama bucket Amazon S3 yang Anda buat.
3. Masukkan jalur tempat Anda ingin snapshot disimpan di dalam ember. Misalnya, **october2023/23**.
4. Pilih Kirim.
5. Setelah lima hingga sepuluh menit, pilih Refresh di halaman Snapshots untuk memeriksa status. Snapshot tidak akan valid sampai status berubah dari IN_PROGRESS menjadi COMPLETED.

Terapkan snapshot

Setelah membuat snapshot lingkungan, Anda dapat menerapkan snapshot tersebut ke lingkungan baru untuk memigrasikan data. Anda perlu menambahkan kebijakan baru ke bucket yang memungkinkan lingkungan membaca snapshot.

Menerapkan snapshot menyalin data seperti izin pengguna, proyek, tumpukan perangkat lunak, profil izin, dan sistem file dengan asosiasi mereka ke lingkungan baru. Sesi pengguna tidak akan direplikasi. Ketika snapshot diterapkan, ia memeriksa informasi dasar dari setiap catatan sumber daya untuk menentukan apakah sudah ada. Untuk rekaman duplikat, snapshot melewati pembuatan sumber daya di lingkungan baru. Untuk catatan yang serupa, seperti berbagi nama atau kunci, tetapi informasi sumber daya dasar lainnya bervariasi, itu akan membuat catatan baru dengan nama dan kunci yang dimodifikasi menggunakan konvensi berikut: RecordName_SnapshotRESVersion_ApplySnapshotID ApplySnapshotIDTampak seperti stempel waktu dan mengidentifikasi setiap upaya untuk menerapkan snapshot.

Selama aplikasi snapshot, snapshot memeriksa ketersediaan sumber daya. Sumber daya yang tidak tersedia untuk lingkungan baru tidak akan dibuat. Untuk sumber daya dengan sumber daya dependen, snapshot memeriksa ketersediaan sumber daya dependen. Jika sumber daya dependen tidak tersedia, itu akan menciptakan sumber daya utama tanpa sumber daya dependen.

Jika lingkungan baru tidak seperti yang diharapkan atau gagal, Anda dapat memeriksa CloudWatch log yang ditemukan di grup log `/res-<env-name>/cluster-manager` untuk detailnya. Setiap log akan memiliki tag `[apply snapshot]`. Setelah Anda menerapkan snapshot, Anda dapat memeriksa statusnya dari [the section called “Manajemen snapshot”](#) halaman.

Untuk menambahkan izin ke bucket:

1. Pilih bucket yang Anda buat dari daftar Bucket.
2. Pilih tab Izin.

3. Di Bawah Kebijakan bucket, pilih Edit.
4. Tambahkan pernyataan berikut ke kebijakan bucket. Ganti nilai-nilai ini dengan nilai Anda sendiri:
 - *111122223333* -> ID AWS Akun Anda
 - *{RES_ENVIRONMENT_NAME}* -> nama lingkungan RES Anda
 - *us-east-1* -> AWS wilayah Anda
 - *amzn-s3-demo-bucket* -> nama ember S3 Anda

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Export-Snapshot-Policy",
      "Effect": "Allow",
      "Principal": {
        "AWS":
          "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
          role-us-east-1}"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
```

```
        "Bool": {
            "aws:SecureTransport": "false"
        },
        "Principal": "*"
    }
}
```

Untuk menerapkan snapshot:

1. Pilih Terapkan snapshot.
2. Masukkan nama bucket Amazon S3 yang berisi snapshot.
3. Masukkan path file ke snapshot di dalam bucket.
4. Pilih Kirim.
5. Setelah lima hingga sepuluh menit, pilih Refresh di halaman manajemen Snapshot untuk memeriksa status.

Bucket Amazon S3

Research and Engineering Studio (RES) mendukung pemasangan [bucket Amazon S3](#) ke instans Linux Virtual Desktop Infrastructure (VDI). Administrator RES dapat memasukkan bucket S3 ke RES, melampirkannya ke proyek, mengedit konfigurasinya, dan menghapus bucket di tab bucket S3 di bawah Manajemen Lingkungan.

Dasbor bucket S3 menyediakan daftar bucket S3 onboard yang tersedia untuk Anda. Dari dasbor bucket S3, Anda dapat:

1. Gunakan Add bucket untuk memasukkan bucket S3 ke RES.
2. Pilih bucket S3 dan gunakan menu Actions untuk:
 - Edit ember
 - Hapus ember
3. Gunakan kolom pencarian untuk mencari berdasarkan nama Bucket dan temukan bucket S3 onboard.

Bagian berikut menjelaskan cara mengelola bucket Amazon S3 di proyek RES Anda.

Topik

- [Prasyarat bucket Amazon S3 untuk penerapan VPC yang terisolasi](#)
- [Tambahkan bucket Amazon S3](#)
- [Edit ember Amazon S3](#)
- [Hapus ember Amazon S3](#)
- [Isolasi Data](#)
- [Akses bucket lintas akun](#)
- [Mencegah eksfiltrasi data dalam VPC pribadi](#)
- [Pemecahan Masalah](#)
- [Mengaktifkan CloudTrail](#)

Prasyarat bucket Amazon S3 untuk penerapan VPC yang terisolasi

Jika Anda menerapkan Research and Engineering Studio di VPC terisolasi, ikuti langkah-langkah berikut untuk memperbarui parameter konfigurasi lambda setelah Anda menerapkan RES di akun Anda. AWS

1. Masuk ke Konsol Lambda AWS akun tempat Studio Penelitian dan Teknik digunakan.
2. Temukan dan arahkan ke fungsi Lambda bernama. *<RES-EnvironmentName>-vdc-custom-credential-broker-lambda*
3. Pilih tab Konfigurasi fungsi.
4. Di sisi kiri, pilih variabel Lingkungan untuk melihat bagian itu.
5. Pilih Edit dan tambahkan variabel lingkungan baru berikut ke fungsi:
 - Kunci: `AWS_STS_REGIONAL_ENDPOINTS`
 - Nilai: `regional`
6. Pilih Simpan.

Tambahkan bucket Amazon S3

Untuk menambahkan bucket S3 ke lingkungan RES Anda:

1. Pilih Tambahkan ember.
2. Masukkan detail bucket seperti nama bucket, ARN, dan mount point.

Important

- Bucket ARN, mount point, dan mode yang disediakan tidak dapat diubah setelah pembuatan.
- Bucket ARN dapat berisi awalan yang akan mengisolasi bucket S3 onboard ke awalan itu.

3. Pilih mode untuk onboard bucket Anda.

Important

- Lihat [Isolasi Data](#) untuk informasi selengkapnya terkait isolasi data dengan mode tertentu.

4. Di bawah Opsi Lanjutan, Anda dapat memberikan ARN peran IAM untuk memasang bucket untuk akses lintas akun. Ikuti langkah-langkah [Akses bucket lintas akun](#) untuk membuat peran IAM yang diperlukan untuk akses lintas akun.
5. (Opsional) Kaitkan bucket dengan proyek, yang dapat diubah nanti. Namun, bucket S3 tidak dapat dipasang ke sesi VDI proyek yang ada. Hanya sesi yang diluncurkan setelah proyek dikaitkan dengan bucket yang akan memasang bucket.
6. Pilih Kirim.

Edit ember Amazon S3

1. Pilih bucket S3 di daftar bucket S3.
2. Dari menu Tindakan, pilih Edit.
3. Masukkan pembaruan Anda.

Important

- Mengaitkan proyek dengan bucket S3 tidak akan memasang bucket ke instance infrastruktur desktop virtual (VDI) proyek yang ada. Bucket hanya akan dipasang ke sesi VDI yang diluncurkan dalam proyek setelah bucket dikaitkan dengan proyek itu.
- Memutuskan hubungan proyek dari bucket S3 tidak akan memengaruhi data di bucket S3, tetapi akan mengakibatkan pengguna desktop kehilangan akses ke data tersebut.

4. Pilih Simpan pengaturan bucket.

Hapus ember Amazon S3

1. Pilih bucket S3 di daftar bucket S3.
2. Dari menu Tindakan, pilih Hapus.

Important

- Anda harus terlebih dahulu menghapus semua asosiasi proyek dari ember.
- Operasi penghapusan tidak memengaruhi data di bucket S3. Ini hanya menghapus asosiasi bucket S3 dengan RES.
- Menghapus bucket akan menyebabkan sesi VDI yang ada kehilangan akses ke konten bucket tersebut setelah berakhirnya kredensial sesi tersebut (~1 jam).

Isolasi Data

Saat menambahkan bucket S3 ke RES, Anda memiliki opsi untuk mengisolasi data di dalam bucket ke proyek dan pengguna tertentu. Pada halaman Add Bucket, Anda dapat memilih mode Read Only (R) atau Read and Write (R/W).

Baca Saja

Jika Read Only (R) dipilih, isolasi data diberlakukan berdasarkan awalan bucket ARN (Nama Sumber Daya Amazon). Misalnya, jika admin menambahkan bucket ke RES menggunakan ARN `arn:aws:s3:::bucket-name/example-data/` dan mengaitkan bucket ini dengan Project A

dan Project B, maka pengguna yang meluncurkan VDIs dari dalam Project A dan Project B hanya dapat membaca data yang terletak di *bucket-name* bawah jalur. */example-data* Mereka tidak akan memiliki akses ke data di luar jalur itu. Jika tidak ada awalan yang ditambahkan ke bucket ARN, seluruh bucket akan tersedia untuk proyek apa pun yang terkait dengannya.

Baca dan Tulis

Jika Read and Write (R/W) dipilih, isolasi data masih diberlakukan berdasarkan awalan bucket ARN, seperti dijelaskan di atas. Mode ini memiliki opsi tambahan untuk memungkinkan administrator memberikan awalan berbasis variabel untuk bucket S3. Saat Read and Write (R/W) dipilih, bagian Awalan Kustom tersedia yang menawarkan menu tarik-turun dengan opsi berikut:

- Tidak ada awalan khusus
- */%p*
- */%p/%u*

Tidak ada isolasi data khusus

Bila No custom prefix dipilih untuk Awalan Kustom, bucket ditambahkan tanpa isolasi data kustom. Ini memungkinkan proyek apa pun yang terkait dengan bucket memiliki akses baca dan tulis. Misalnya, jika admin menambahkan bucket ke RES menggunakan ARN `arn:aws:s3:::bucket-name` dengan yang No custom prefix dipilih dan mengaitkan bucket ini dengan Project A dan Project B, pengguna yang meluncurkan VDIs dari dalam Project A dan Project B akan memiliki akses baca dan tulis yang tidak terbatas ke bucket.

Isolasi data pada tingkat per proyek

Bila */%p* dipilih untuk Awalan Kustom, data dalam bucket diisolasi ke setiap proyek tertentu yang terkait dengannya. *%p* Variabel mewakili kode proyek. Misalnya, jika admin menambahkan bucket ke RES menggunakan ARN `arn:aws:s3:::bucket-name` dengan yang */%p* dipilih dan Mount Point of */bucket*, dan mengaitkan bucket ini dengan Project A dan Project B, maka Pengguna A di Project A dapat menulis file ke */bucket* Pengguna B di Proyek A juga dapat melihat file yang ditulis Pengguna A */bucket*. Namun, jika Pengguna B meluncurkan VDI di Proyek B dan melihat ke dalam */bucket*, mereka tidak akan melihat file yang ditulis Pengguna A, karena data diisolasi oleh proyek. File yang ditulis Pengguna A ditemukan di bucket S3 di bawah awalan */ProjectA* sementara Pengguna B hanya dapat mengakses */ProjectB* saat menggunakan file VDIs dari Project B.

Isolasi data pada tingkat per proyek, per pengguna

Bila `/%p/%u` dipilih untuk Awalan Kustom, data dalam bucket diisolasi ke setiap proyek tertentu dan pengguna yang terkait dengan proyek tersebut. `%p` Variabel mewakili kode proyek, dan `%u` mewakili nama pengguna. Misalnya, admin menambahkan bucket ke RES menggunakan ARN `arn:aws:s3:::bucket-name` dengan `/%p/%u` dipilih dan Mount Point of. `/i>bucket` Bucket ini dikaitkan dengan Project A dan Project B. Pengguna A di Project A dapat menulis file ke `/i>bucket`. Berbeda dengan skenario sebelumnya dengan hanya `%p` isolasi, Pengguna B dalam hal ini tidak akan melihat file yang ditulis Pengguna A di Proyek A/`i>bucket`, karena data diisolasi oleh proyek dan pengguna. File yang ditulis Pengguna A ditemukan di bucket S3 di bawah awalan `/ProjectA/UserA` sementara Pengguna B hanya dapat mengakses `/ProjectA/UserB` saat menggunakannya VDI di Project A.

Akses bucket lintas akun

RES memiliki kemampuan untuk memasang bucket dari AWS akun lain, asalkan bucket ini memiliki izin yang tepat. Dalam skenario berikut, lingkungan RES di Akun A ingin memasang bucket S3 di Akun B.

Langkah 1: Buat Peran IAM di akun tempat RES digunakan (ini akan disebut sebagai Akun A):

1. Masuk ke Konsol AWS Manajemen untuk akun RES yang memerlukan akses ke bucket S3 (Akun A).
2. Buka Konsol IAM:
 - a. Arahkan ke dasbor IAM.
 - b. Di panel navigasi, pilih Kebijakan.
3. Buat Kebijakan:
 - a. Pilih Buat kebijakan.
 - b. Pilih tab JSON.
 - c. Tempel kebijakan JSON berikut (ganti `amzn-s3-demo-bucket` dengan nama bucket S3 yang terletak di Akun B):

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:ListBucket",
      "s3:DeleteObject",
      "s3:AbortMultipartUpload"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  }
]
```

- d. Pilih Berikutnya.
4. Tinjau dan buat kebijakan:
 - a. Berikan nama untuk kebijakan (misalnya, "S3 AccessPolicy").
 - b. Tambahkan deskripsi opsional untuk menjelaskan tujuan kebijakan.
 - c. Tinjau kebijakan dan pilih Buat kebijakan.
5. Buka Konsol IAM:
 - a. Arahkan ke dasbor IAM.
 - b. Di panel navigasi, pilih Peran.
6. Buat Peran:
 - a. Pilih Buat peran.
 - b. Pilih Kebijakan kepercayaan khusus sebagai jenis entitas tepercaya.
 - c. Rekatkan kebijakan JSON berikut (ganti **111122223333** dengan ID akun A yang sebenarnya, **<ENVIRONMENT_NAME>** dengan nama lingkungan penerapan RES, dan **us-east-1** dengan AWS wilayah RES digunakan):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS":
          "arn:aws:iam::11112223333:role/<ENVIRONMENT_NAME>-custom-credential-
broker-lambda-role-us-east-1"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- d. Pilih Berikutnya.
7. Lampirkan Kebijakan Izin:
 - a. Cari dan pilih kebijakan yang Anda buat sebelumnya.
 - b. Pilih Berikutnya.
8. Tandai, Tinjau, dan Buat Peran:
 - a. Masukkan nama peran (misalnya, "S3 AccessRole").
 - b. Di bawah Langkah 3, pilih Tambahkan Tag, lalu masukkan kunci dan nilai berikut:
 - Kunci: `res:Resource`
 - Nilai: `s3-bucket-iam-role`
 - c. Tinjau peran dan pilih Buat peran.
9. Gunakan Peran IAM di RES:
 - a. Salin peran IAM ARN yang Anda buat.
 - b. Masuk ke konsol RES.
 - c. Di panel navigasi kiri, pilih S3 Bucket.
 - d. Pilih Add Bucket dan isi formulir dengan bucket S3 lintas akun ARN.
 - e. Pilih Pengaturan lanjutan - dropdown opsional.

- f. Masukkan peran ARN di bidang ARN peran IAM.
- g. Pilih Tambahkan Ember.

Langkah 2: Ubah kebijakan bucket di Akun B

1. Masuk ke Konsol AWS Manajemen untuk Akun B.
2. Buka Konsol S3:
 - a. Arahkan ke dasbor S3.
 - b. Pilih bucket yang ingin Anda berikan aksesnya.
3. Edit Kebijakan Bucket:
 - a. Pilih tab Izin dan pilih Kebijakan Bucket.
 - b. Tambahkan kebijakan berikut untuk memberikan peran IAM dari Akun A akses ke bucket (ganti **111122223333** dengan ID akun aktual Akun A dan **amzn-s3-demo-bucket** dengan nama bucket S3):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

```
}  
]
```

- c. Pilih Simpan.

Mencegah eksfiltrasi data dalam VPC pribadi

Untuk mencegah pengguna mengeksfiltrasi data dari bucket S3 aman ke bucket S3 mereka sendiri di akun mereka, Anda dapat melampirkan titik akhir VPC untuk mengamankan VPC pribadi Anda. Langkah-langkah berikut menunjukkan cara membuat titik akhir VPC untuk layanan S3 yang mendukung akses ke bucket S3 di dalam akun Anda, serta akun tambahan apa pun yang memiliki bucket lintas akun.

1. Buka Konsol VPC Amazon:
 - a. Masuk ke Konsol AWS Manajemen.
 - b. Buka konsol VPC Amazon di <https://console.aws.amazon.com/vpc/>
2. Buat Endpoint VPC untuk S3:
 - a. Pada panel navigasi kiri, pilih Titik Akhir.
 - b. Pilih Buat Titik Akhir.
 - c. Untuk kategori Layanan, pastikan bahwa AWS layanan dipilih.
 - d. Di bidang Nama Layanan, masukkan `com.amazonaws.<region>.s3` (ganti `<region>` dengan AWS wilayah Anda) atau cari "S3".
 - e. Pilih layanan S3 dari daftar.
3. Konfigurasi Pengaturan Titik Akhir:
 - a. Untuk VPC, pilih VPC tempat Anda ingin membuat titik akhir.
 - b. Untuk Subnet, pilih kedua subnet pribadi yang digunakan untuk Subnet VDI selama penerapan.
 - c. Untuk Aktifkan nama DNS, pastikan opsi dicentang. Ini memungkinkan nama host DNS pribadi diselesaikan ke antarmuka jaringan titik akhir.
4. Konfigurasi Kebijakan untuk Membatasi Akses:
 - a. Di bawah Kebijakan, pilih Kustom.
 - b. Di editor kebijakan, masukkan kebijakan yang membatasi akses ke sumber daya dalam akun Anda atau akun tertentu. Berikut adalah contoh kebijakan (ganti `amzn-s3-demo-`

bucket dengan nama bucket S3 Anda dan **111122223333** dan **444455556666** dengan AWS akun yang sesuai IDs yang ingin Anda akses):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [
            "111122223333",
            "444455556666"
          ]
        }
      }
    }
  ]
}
```

5. Buat Endpoint:

- a. Meninjau pengaturan Anda.
- b. Pilih Buat titik akhir.

6. Verifikasi Endpoint:

- a. Setelah titik akhir dibuat, navigasikan ke bagian Endpoints di konsol VPC.
- b. Pilih endpoint yang baru dibuat.
- c. Verifikasi bahwa Negara Tersedia.

Dengan mengikuti langkah-langkah ini, Anda membuat titik akhir VPC yang memungkinkan akses S3 yang dibatasi untuk sumber daya dalam akun Anda atau ID akun tertentu.

Pemecahan Masalah

Cara memeriksa apakah ember gagal dipasang pada VDI

Jika bucket gagal dipasang pada VDI, ada beberapa lokasi di mana Anda dapat memeriksa kesalahan. Ikuti langkah-langkah di bawah ini.

1. Periksa Log VDI:

- a. Masuk ke Konsol AWS Manajemen.
- b. Buka EC2 Konsol dan arahkan ke Instans.
- c. Pilih instance VDI yang Anda luncurkan.
- d. Connect ke VDI melalui Session Manager.
- e. Jalankan perintah berikut:

```
sudo su
cd ~/bootstrap/logs
```

Di sini, Anda akan menemukan log bootstrap. Rincian kegagalan apa pun akan ditemukan di `configure.log.{time}` file.

Selain itu, periksa `/etc/message log` untuk lebih jelasnya.

2. Periksa Log CloudWatch Lambda Broker Kredensi Kustom:

- a. Masuk ke Konsol AWS Manajemen.
- b. Buka CloudWatch Konsol dan arahkan ke Grup log.
- c. Cari grup log `aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.
- d. Periksa grup log pertama yang tersedia dan temukan kesalahan apa pun di dalam log. Log ini akan berisi detail mengenai potensi masalah yang menyediakan kredensial khusus sementara untuk memasang bucket S3.

3. Periksa CloudWatch Log API Gateway API Credential Kustom:

- a. Masuk ke Konsol AWS Manajemen.
- b. Buka CloudWatch Konsol dan arahkan ke Grup log.
- c. Cari grup log `<stack-name>-vdc-custom-credential-broker-lambda vdc custom credential broker api gateway access logs <nonce>`.

- d. Periksa grup log pertama yang tersedia dan temukan kesalahan apa pun di dalam log. Log ini akan berisi detail mengenai permintaan dan tanggapan apa pun terhadap API Gateway untuk kredensyal khusus yang diperlukan untuk memasang bucket S3.

Cara mengedit konfigurasi peran IAM bucket setelah onboarding

1. Masuk ke Konsol [AWS DynamoDB](#).
2. Pilih Tabel:
 - a. Di panel navigasi kiri, pilih Tabel.
 - b. Temukan dan pilih `<stack-name>.cluster-settings`.
3. Pindai Tabel:
 - a. Pilih Jelajahi item tabel.
 - b. Pastikan Pemindaian dipilih.
4. Tambahkan Filter:
 - a. Pilih Filter untuk membuka bagian entri filter.
 - b. Atur filter agar sesuai dengan kunci Anda-
 - Atribut: Masukkan kunci.
 - Kondisi: Pilih Dimulai dengan.
 - Nilai: Masukkan `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` penggantian `<filesystem_id>` dengan nilai sistem file yang perlu dimodifikasi.
5. Jalankan Pemindaian:

Pilih Jalankan untuk menjalankan pemindaian dengan filter.
6. Periksa nilainya:

Jika entri ada, pastikan nilainya diatur dengan benar dengan ARN peran IAM yang tepat.

Jika entri tidak ada:

 - a. Pilih Buat item.
 - b. Masukkan detail item:

- Untuk atribut kunci, masukkan `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
 - Tambahkan ARN peran IAM yang benar.
- c. Pilih Simpan untuk menambahkan item.
7. Mulai ulang instance VDI:
- Reboot instance untuk memastikan VDIs yang terpengaruh oleh peran IAM yang salah ARN dipasang lagi.

Mengaktifkan CloudTrail

Untuk mengaktifkan CloudTrail di akun Anda menggunakan CloudTrail konsol, ikuti petunjuk yang disediakan di [Membuat jejak dengan CloudTrail konsol](#) di Panduan AWS CloudTrail Pengguna.

CloudTrail akan mencatat akses ke bucket S3 dengan merekam peran IAM yang mengaksesnya. Ini dapat ditautkan kembali ke ID instance, yang ditautkan ke proyek atau pengguna.

Gunakan produk

Bagian ini menawarkan panduan kepada pengguna tentang penggunaan desktop virtual untuk berkolaborasi dengan pengguna lain.

Topik

- [Akses SSH](#)
- [Desktop virtual](#)
- [Desktop bersama](#)
- [Browser file](#)

Akses SSH

Untuk menggunakan SSH untuk mengakses host bastion:

1. Dari menu RES, pilih akses SSH.
2. Ikuti petunjuk di layar untuk menggunakan SSH atau PuTTY untuk akses.

Desktop virtual

Modul antarmuka desktop virtual (VDI) memungkinkan pengguna membuat dan mengelola desktop virtual Windows atau Linux. AWS Pengguna dapat meluncurkan EC2 instans Amazon dengan alat dan aplikasi favorit mereka yang sudah diinstal sebelumnya dan dikonfigurasi.

Sistem operasi yang didukung

RES saat ini mendukung peluncuran desktop virtual menggunakan sistem operasi berikut:

- Amazon Linux 2 (x86 dan ARM64)
- Ubuntu 22.04.03 (x86)
- RHEL 8 (x86), dan 9 (x86)
- Windows 2019, 2022 (x86)

Topik

- [Luncurkan desktop baru](#)

- [Akses desktop Anda](#)
- [Kontrol status desktop Anda](#)
- [Memodifikasi desktop virtual](#)
- [Ambil informasi sesi](#)
- [Jadwalkan desktop virtual](#)
- [Antarmuka desktop virtual autostop](#)

Luncurkan desktop baru

1. Dari menu, pilih My Virtual Desktops.
2. Pilih Luncurkan Desktop Virtual Baru.
3. Masukkan detail untuk desktop baru Anda.
4. Pilih Kirim.

Kartu baru dengan informasi desktop Anda muncul secara instan, dan desktop Anda akan siap digunakan dalam waktu 10-15 menit. Waktu startup tergantung pada gambar yang dipilih. RES mendeteksi instans GPU dan menginstal driver yang relevan.

Akses desktop Anda

Untuk mengakses desktop virtual, pilih kartu untuk desktop dan sambungkan menggunakan web atau klien DCV.

Web connection

Mengakses desktop Anda melalui browser web adalah metode koneksi termudah.

- Pilih Connect, atau pilih thumbnail untuk mengakses desktop Anda secara langsung melalui browser Anda.

DCV connection

Mengakses desktop Anda melalui klien DCV menawarkan kinerja terbaik. Untuk mengakses melalui DCV:

1. Pilih File Sesi DCV untuk mengunduh .dcv file. Anda akan memerlukan klien DCV yang diinstal pada sistem Anda.
2. Untuk petunjuk instalasi, pilih? ikon.

Kontrol status desktop Anda

Untuk mengontrol status desktop Anda:

1. Pilih Tindakan.
2. Pilih Status Desktop Virtual. Anda memiliki empat negara untuk dipilih:

- Berhenti

Sesi yang berhenti tidak akan mengalami kehilangan data, dan Anda dapat memulai ulang sesi yang dihentikan kapan saja.

- Reboot

Reboot sesi saat ini.

- Mengakhiri

Mengakhiri sesi secara permanen. Mengakhiri sesi dapat menyebabkan kehilangan data jika Anda menggunakan penyimpanan sementara. Anda harus mencadangkan data Anda ke sistem file RES sebelum mengakhiri.

- Hibernasi

Status desktop Anda akan disimpan dalam memori. Saat Anda me-restart desktop, aplikasi Anda akan dilanjutkan tetapi koneksi jarak jauh apa pun mungkin terputus. Tidak semua instance mendukung hibernasi, dan opsi hanya tersedia jika diaktifkan selama pembuatan instance. Untuk memverifikasi apakah instans Anda mendukung status ini, lihat Prasyarat [hibernasi](#).

Memodifikasi desktop virtual

Anda dapat memperbarui perangkat keras desktop virtual Anda atau mengubah nama sesi.

1. Sebelum membuat perubahan pada ukuran instans, Anda harus menghentikan sesi:
 - a. Pilih Tindakan.
 - b. Pilih Status Desktop Virtual.
 - c. Pilih Berhenti.

 Note

Anda tidak dapat memperbarui ukuran desktop untuk sesi hibernasi.

2. Setelah Anda mengonfirmasi desktop telah berhenti, pilih Tindakan dan kemudian pilih Perbarui Sesi.
3. Ubah nama sesi atau pilih ukuran desktop yang Anda inginkan.
4. Pilih Kirim.
5. Setelah instans Anda diperbarui, restart desktop Anda:
 - a. Pilih Tindakan.
 - b. Pilih Status Desktop Virtual.
 - c. Pilih Mulai.

Ambil informasi sesi

1. Pilih Tindakan.
2. Pilih Tampilkan Info.

Jadwalkan desktop virtual

Secara default, desktop virtual tidak memiliki jadwal dan akan tetap aktif sampai Anda menghentikan atau mengakhiri sesi. Desktop juga berhenti jika idle untuk mencegah berhenti secara tidak sengaja. Keadaan idle ditentukan oleh tidak ada koneksi aktif dan penggunaan CPU di bawah 15% selama setidaknya 15 menit. Anda dapat mengonfigurasi jadwal untuk memulai dan menghentikan desktop Anda secara otomatis.

1. Pilih Tindakan.
2. Pilih Jadwal.
3. Atur jadwal Anda untuk setiap hari.
4. Pilih Simpan.

Antarmuka desktop virtual autostop

Administrator dapat mengonfigurasi pengaturan untuk memungkinkan idle VDI's Dihentikan atau Dihentikan. Ada 4 pengaturan yang dapat dikonfigurasi:

1. Idle Timeout: Sesi idle untuk kali ini dengan pemanfaatan CPU di bawah ambang batas akan habis.
2. Ambang Pemanfaatan CPU: Sesi tanpa interaksi dan di bawah ambang batas ini dianggap menganggur. Jika ini diatur ke 0, maka sesi tidak akan pernah dianggap idle.
3. Status Transisi: Setelah batas waktu idle, sesi akan beralih ke status ini (dihentikan atau dihentikan).
4. Menegakkan Jadwal: Jika dipilih, sesi yang telah dihentikan karena menganggur dapat dilanjutkan dengan jadwal hariannya.

Pengaturan ini ada di halaman Pengaturan Desktop di bawah tab Server. Setelah Anda memperbarui pengaturan sesuai dengan kebutuhan Anda, klik Kirim untuk menyimpan pengaturan. Sesi baru akan menggunakan pengaturan yang diperbarui, tetapi perhatikan bahwa sesi yang ada masih akan menggunakan pengaturan yang mereka miliki saat diluncurkan.

Setelah waktu habis, sesi akan berakhir atau bertransisi ke STOPPED_IDLE status berdasarkan konfigurasinya. Pengguna akan memiliki kemampuan untuk memulai STOPPED_IDLE sesi dari UI.

Desktop bersama

Di Desktop Bersama, Anda dapat melihat desktop yang telah dibagikan dengan Anda. Untuk terhubung ke desktop, pemilik sesi harus terhubung juga kecuali Anda adalah Admin atau Pemilik.

Saat berbagi sesi, Anda dapat mengonfigurasi izin untuk kolaborator Anda. Misalnya, Anda dapat memberikan akses hanya-baca ke rekan satu tim dengan siapa Anda berkolaborasi.

Topik

- [Bagikan desktop](#)
- [Mengakses desktop bersama](#)

Bagikan desktop

1. Dari sesi desktop Anda, pilih Tindakan.
2. Pilih Izin Sesi.
3. Pilih tingkat pengguna dan izin. Anda juga dapat menetapkan waktu kedaluwarsa.
4. Pilih Simpan.

Untuk informasi selengkapnya tentang izin, lihat [the section called “Kebijakan izin”](#).

Mengakses desktop bersama

Dari Shared Desktops, Anda dapat melihat desktop yang dibagikan dengan Anda dan terhubung ke sebuah instans. Anda dapat bergabung dengan browser web atau DCV. Untuk terhubung, ikuti petunjuk di [Akses desktop Anda](#).

Browser file

File browser memungkinkan Anda untuk mengakses filesystem melalui portal web. Anda dapat mengelola semua file yang tersedia yang memiliki izin untuk diakses pada sistem file yang mendasarinya. Penyimpanan backend (Amazon EFS) tersedia untuk semua node Linux. Untuk node Linux dan Windows, FSx untuk ONTAP tersedia. Memperbarui file di desktop virtual Anda sama dengan memperbarui file melalui terminal atau browser file berbasis web.

Topik

- [Unggah file](#)
- [Hapus berkas](#)

- [Kelola favorit](#)
- [Mengedit file](#)
- [Transfer file](#)

Unggah file

1. Pilih Unggah file.
2. Jatuhkan file atau telusuri file untuk diunggah.
3. Pilih Unggah (n) file.

Hapus berkas

1. Pilih file yang ingin Anda hapus.
2. Pilih Tindakan.
3. Pilih Hapus file.

Atau, Anda juga dapat mengklik kanan file atau folder apa pun dan memilih Hapus file.

Kelola favorit

Untuk menyematkan file dan folder penting, Anda dapat menambahkannya ke Favorit.

1. Pilih file atau folder.
2. Pilih Favorit.

Atau, Anda dapat mengklik kanan file atau folder apa pun dan memilih Favorit.

Note

Favorit disimpan ke browser lokal. Jika Anda mengubah browser atau menghapus cache, Anda harus menyematkan ulang favorit Anda.

Mengedit file

Anda dapat mengedit konten file berbasis teks dalam portal web.

1. Pilih file yang ingin Anda perbarui. Modal akan terbuka dengan konten file.
2. Buat pembaruan Anda dan pilih Simpan.

Transfer file

Gunakan Transfer File untuk menggunakan aplikasi transfer file eksternal untuk mentransfer file. Anda dapat memilih dari aplikasi berikut dan mengikuti petunjuk di layar untuk mentransfer file.

- FileZilla (Windows, macOS, Linux)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)

Pemecahan Masalah

Bagian ini berisi informasi tentang cara memantau sistem dan cara memecahkan masalah tertentu yang mungkin terjadi.

Topik

- [Debugging dan Pemantauan Umum](#)
- [Masalah RunBooks](#)
- [Masalah yang Diketahui](#)

Isi terperinci:

- [Debugging dan Pemantauan Umum](#)
 - [Sumber informasi log dan peristiwa yang berguna](#)
 - [Log file di lingkungan EC2 instans Amazon](#)
 - [CloudFormation Tumpukan](#)
 - [Kegagalan sistem karena masalah dan tercermin oleh Aktivitas Grup EC2 Auto Scaling Amazon](#)
 - [Penampilan EC2 Konsol Amazon Khas](#)
 - [Infrastruktur host](#)
 - [Infrastruktur host dan virtual desktop](#)
 - [Host dalam keadaan dihentikan](#)
 - [Perintah terkait Active Directory \(AD\) yang berguna untuk referensi](#)
 - [Debugging Windows DCV](#)
 - [Temukan Informasi Versi Amazon DCV](#)
- [Masalah RunBooks](#)
 - [Masalah instalasi](#)
 - [Saya ingin mengatur domain khusus setelah saya menginstal RES](#)
 - [AWS CloudFormation tumpukan gagal dibuat dengan pesan "WaitCondition menerima pesan gagal. Kesalahan:Negara. TaskFailed"](#)
 - [Pemberitahuan email tidak diterima setelah AWS CloudFormation tumpukan berhasil dibuat](#)
 - [Instance bersepeda atau vdc-controller dalam keadaan gagal](#)

- [CloudFormation Tumpukan lingkungan gagal dihapus karena kesalahan objek dependen](#)
- [Kesalahan ditemui untuk parameter blok CIDR selama pembuatan lingkungan](#)
- [CloudFormation kegagalan pembuatan tumpukan selama pembuatan lingkungan](#)
- [Pembuatan tumpukan sumber daya eksternal \(demo\) gagal dengan AdDomainAdminNode CREATE_FAILED](#)
- [Masalah manajemen identitas](#)
 - [Saya tidak berwenang untuk melakukan iam: PassRole](#)
 - [Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses Studio Penelitian dan Teknik saya tentang AWS sumber daya](#)
 - [Saat masuk ke lingkungan, saya segera kembali ke halaman login](#)
 - [Kesalahan “Pengguna tidak ditemukan” saat mencoba masuk](#)
 - [Pengguna ditambahkan di Active Directory, tetapi hilang dari RES](#)
 - [Pengguna tidak tersedia saat membuat sesi](#)
 - [Batas ukuran melebihi kesalahan dalam log CloudWatch pengelola kluster](#)
- [Penyimpanan](#)
 - [Saya membuat sistem file melalui RES tetapi tidak dipasang di host VDI](#)
 - [Saya memasukkan sistem file melalui RES tetapi tidak dipasang di host VDI](#)
 - [Saya tidak dapat mengaktifkan read/write dari host VDI](#)
 - [Contoh izin menangani kasus penggunaan](#)
 - [Saya membuat Amazon FSx untuk NetApp ONTAP dari RES tetapi tidak bergabung dengan domain saya](#)
- [Snapshot](#)
 - [Snapshot memiliki status Gagal](#)
 - [Snapshot gagal diterapkan dengan log yang menunjukkan bahwa tabel tidak dapat diimpor.](#)
- [Infrastruktur](#)
 - [Kelompok sasaran penyeimbang beban tanpa instance yang sehat](#)
- [Meluncurkan Desktop Virtual](#)
 - [Desktop virtual yang sebelumnya berfungsi tidak lagi dapat terhubung dengan sukses](#)
 - [Saya hanya dapat meluncurkan 5 desktop virtual](#)
- [Upaya koneksi Windows Desktop gagal dengan “Koneksi telah ditutup. Kesalahan transportasi”](#)

- [VDIs terjebak dalam status Penyediaan](#)
- [VDIs masuk ke status Kesalahan setelah diluncurkan](#)
- [Komponen Desktop Virtual](#)
 - [EC2 Instans Amazon berulang kali ditampilkan dihentikan di konsol](#)
 - [instance vdc-controller sedang bersepeda karena gagal bergabung dengan modul AD/eVDi menunjukkan Pemeriksaan Kesehatan API Gagal](#)
 - [Proyek tidak muncul di pull down saat mengedit Software Stack untuk menambahkannya](#)
 - [pengelola klaster Log CloudWatch Amazon menunjukkan “user-home-init< > akun belum tersedia. menunggu pengguna untuk disinkronkan” \(di mana akun adalah nama pengguna\)](#)
 - [Desktop Windows pada upaya login mengatakan “Akun Anda telah dinonaktifkan. Silakan lihat administrator Anda”](#)
 - [Masalah Opsi DHCP dengan konfigurasi external/customer AD](#)
 - [Kesalahan Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING](#)
- [Penghapusan Env](#)
 - [res-xxx-cluster tumpuk dalam status “DELETE_FAILED” dan tidak dapat dihapus secara manual karena kesalahan “Peran tidak valid atau tidak dapat diasumsikan”](#)
 - [Mengumpulkan Log](#)
 - [Mengunduh VDI Logs](#)
 - [Mengunduh log dari EC2 instance Linux](#)
 - [Mengunduh log dari EC2 instance Windows](#)
 - [Mengumpulkan log ECS untuk kesalahan WaitCondition](#)
- [Lingkungan demo](#)
 - [Kesalahan login lingkungan demo saat menangani permintaan otentikasi ke penyedia identitas](#)
 - [Demo stack keycloak tidak berfungsi](#)
- [Masalah yang Diketahui 2024.x](#)
 - [Masalah yang Diketahui 2024.x](#)
 - [\(2024.08\) Desktop virtual gagal memasang bucket Amazon S3 read/write dengan root bucket ARN dan awalan khusus](#)
 - [\(2024.06\) Menerapkan snapshot gagal saat nama grup AD berisi spasi](#)
 - [\(2024.04-2024.04.02\) Memberikan Batas Izin IAM yang tidak dilampirkan ke peran instans VDI](#)

- [\(2024.04.02 dan sebelumnya\) Instans Windows NVIDIA di ap-southeast-2 \(Sydney\) gagal diluncurkan](#)
- [\(2024.04 dan 2024.04.01\) Kegagalan penghapusan RES di GovCloud](#)
- [\(2024.04 - 2024.04.02\) Desktop virtual Linux mungkin macet dalam status “MELANJUTKAN” saat reboot](#)
- [\(2024.04.02 dan sebelumnya\) Gagal menyinkronkan pengguna AD yang atribut SAMAccount Namanya menyertakan huruf kapital atau karakter khusus](#)
- [\(2024.04.02 dan sebelumnya\) Kunci pribadi untuk mengakses host bastion tidak valid](#)
- [\(2024.06 dan sebelumnya\) Anggota grup tidak disinkronkan ke RES selama sinkronisasi AD](#)
- [\(2024.06 dan sebelumnya\) CVE-2024-6387, Regre, Kerentanan Keamanan di dan Ubuntu SSHion RHEL9 VDI](#)

Debugging dan Pemantauan Umum

Bagian ini berisi informasi tentang di mana informasi dapat ditemukan dalam RES.

- [Sumber informasi log dan peristiwa yang berguna](#)
 - [Log file di lingkungan EC2 instans Amazon](#)
 - [CloudFormation Tumpukan](#)
 - [Kegagalan sistem karena masalah dan tercermin oleh Aktivitas Grup EC2 Auto Scaling Amazon](#)
- [Penampilan EC2 Konsol Amazon Khas](#)
 - [Infrastruktur host](#)
 - [Infrastruktur host dan virtual desktop](#)
 - [Host dalam keadaan dihentikan](#)
 - [Perintah terkait Active Directory \(AD\) yang berguna untuk referensi](#)
- [Debugging Windows DCV](#)
- [Temukan Informasi Versi Amazon DCV](#)

Sumber informasi log dan peristiwa yang berguna

Ada berbagai sumber informasi yang disimpan yang dapat direferensikan untuk pemecahan masalah dan pemantauan penggunaan.

Log file di lingkungan EC2 instans Amazon

File log ada di EC2 instans Amazon yang digunakan oleh RES. SSM Session Manager dapat digunakan untuk membuka sesi ke instance untuk memeriksa file-file ini.

Pada instance infrastruktur seperti cluster-manager dan vdc-controller, aplikasi dan log lainnya dapat ditemukan di lokasi berikut.

- /opt/idea/app/logs/application.log
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssdl/
- /var/log/messages
- /var/log/user-data.log
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

Pada desktop virtual Linux, berikut ini berisi file log yang berguna

- /var/log/dcv/
- /root/bootstrap/logs/userdata.log
- /var/log/messages

Pada Windows virtual desktop instance log dapat ditemukan di

- PS C:\ProgramData\nes\ dcv\ log
- PS C:\ProgramData\nes\ DCVSessionManagerAgent\ log

Pada Windows, beberapa aplikasi logging dapat ditemukan di:

- PS C:\Program File\ BAGUS\ DCV\ Server\ bin

Di Windows, file sertifikat NICE DCV dapat ditemukan di:

- C:\Windows\System32\config\systemprofile\AppData\ Lokal\ BAGUS\ dcv\

Grup CloudWatch Log Amazon

Amazon EC2 dan AWS Lambda menghitung informasi log sumber daya ke Amazon CloudWatch Log Groups. Entri log di dalamnya dapat memberikan informasi yang berguna saat memecahkan masalah potensial atau untuk informasi umum.

Kelompok-kelompok tersebut diberi nama sebagai berikut:

- `/aws/lambda/<envname>-/` - lambda related
- `/<envname>/`
 - `cluster-manager/` - main infrastructure host
 - `vdc/` - virtual desktop related
 - `dcv-broker/` - desktop related
 - `dcv-connection-gateway/` - desktop related
 - `controller/` - main desktop controller host
 - `dcv-session/` - desktop session related

Saat memeriksa grup log, akan sangat membantu untuk memfilter menggunakan string huruf besar dan kecil seperti berikut ini. Ini hanya akan menampilkan pesan-pesan yang berisi string yang dicatat.

```
?"ERROR" ?"error"
```

Metode pemantauan lain untuk masalah adalah membuat CloudWatch Dasbor Amazon yang berisi widget yang menampilkan data yang menarik.

Contohnya adalah membuat widget yang menghitung terjadinya kesalahan string dan ERROR dan grafiknya sebagai garis. Metode ini memudahkan untuk mendeteksi terjadinya potensi masalah atau tren yang menunjukkan perubahan pola telah terjadi.

Berikut ini adalah contoh untuk host infrastruktur. Untuk menggunakan ini, menggabungkan baris query dan mengganti `<envname>` dan `<region>` atribut dengan nilai-nilai yang sesuai.

```
{
  "widgets": [
    {
      "type": "log",
      "x": 0,
      "y": 0,
```

```

    "width": 24,
    "height": 6,
    "properties": {
      "query": "SOURCE '/<envname>/vdc/controller' |
        SOURCE '/<envname>/cluster-manager' |
        SOURCE '/<envname>/vdc/dcv-broker' |
        SOURCE '/<envname>/vdc/dcv-connection-gateway' |
        fields @timestamp, @message, @logStream, @log\n|
        filter @message like /(?(i)(error|ERROR))/\n|
        sort @timestamp desc|
        stats count() by bin(30s)",
      "region": "<region>",
      "title": "infrastructure hosts",
      "view": "timeSeries",
      "stacked": false
    }
  }
]
}

```

Contoh Dashboard mungkin muncul sebagai berikut:

CloudFormation Tumpukan

CloudFormation Tumpukan yang dibuat selama pembuatan lingkungan berisi sumber daya, peristiwa, dan informasi keluaran yang terkait dengan konfigurasi lingkungan.

Untuk setiap tumpukan, tab Acara, Sumber Daya, dan Keluaran dapat dirujuk untuk informasi tentang tumpukan.

Tumpukan RES:

- <envname>-bootstrap
- <envname>-kluster
- <envname>-metrik
- <envname>-layanan direktori
- <envname>-penyedia identitas
- <envname>-penyimpanan bersama
- <envname>-pengelola-klaster

- `<envname>-vdc`
- `<envname>-bastion-host`

Tumpukan Lingkungan Demo (Jika Anda menerapkan lingkungan demo dan tidak memiliki sumber daya eksternal ini, Anda dapat menggunakan resep Komputasi Kinerja AWS Tinggi untuk menghasilkan sumber daya untuk lingkungan demo.)

- `<envname>`
- `<envname>-Jaringan`
- `<envname>-DirectoryService`
- `<envname>-Penyimpanan`
- `<envname>-WindowsManagementHost`

Kegagalan sistem karena masalah dan tercermin oleh Aktivitas Grup EC2 Auto Scaling Amazon

Jika RES UIs menunjukkan kesalahan server, penyebabnya mungkin perangkat lunak aplikasi atau masalah lainnya.

Setiap infrastruktur Amazon EC2 instance autoscaling groups (ASGs) berisi tab Activity yang dapat berguna untuk mendeteksi aktivitas penskalaan untuk instance. Jika halaman UI mencatat kesalahan apa pun atau tidak dapat diakses, periksa EC2 konsol Amazon untuk beberapa instance yang dihentikan dan periksa tab Aktivitas Grup Penskalaan Otomatis untuk ASG terkait untuk menentukan apakah instans Amazon EC2 sedang bersepeda.

Jika demikian, gunakan grup CloudWatch log Amazon terkait untuk instans untuk menentukan apakah kesalahan sedang dicatat yang mungkin menunjukkan penyebab masalah. Dimungkinkan juga untuk menggunakan konsol Sesi SSM untuk membuka sesi ke instance yang sedang berjalan dari jenis itu dan memeriksa file log pada instance untuk menentukan penyebab sebelum instance ditandai sebagai tidak sehat dan dihentikan oleh ASG.

Konsol ASG dapat menampilkan aktivitas yang mirip dengan berikut ini jika masalah ini terjadi.

Penampilan EC2 Konsol Amazon Khas

Bagian ini berisi tangkapan layar dari sistem yang beroperasi di berbagai negara bagian.

Infrastruktur host

EC2 Konsol Amazon, ketika tidak ada desktop yang berjalan, biasanya terlihat mirip dengan yang berikut ini. Contoh yang ditampilkan adalah infrastruktur RES EC2 host Amazon. Awalan dalam nama instance adalah nama lingkungan RES.

Infrastruktur host dan virtual desktop

Di EC2 konsol Amazon, ketika desktop virtual berjalan, mereka tampak mirip dengan yang berikut ini. Dalam hal ini, desktop virtual dicatat dengan warna merah. Sufiks untuk nama instance adalah pengguna yang membuat desktop. Nama di tengah adalah Nama Sesi yang ditetapkan pada waktu peluncuran dan merupakan default "MyDesktop" atau nama yang ditetapkan oleh pengguna.

Host dalam keadaan dihentikan

Ketika EC2 konsol Amazon menampilkan instance yang dihentikan, mereka umumnya host desktop yang telah dihentikan. Jika konsol menyertakan host infrastruktur dalam status dihentikan, terutama jika ada beberapa dari jenis yang sama, itu mungkin menunjukkan masalah sistem sedang berlangsung.

Gambar berikut menunjukkan instance desktop yang telah dihentikan.

Perintah terkait Active Directory (AD) yang berguna untuk referensi

Berikut ini adalah contoh perintah terkait ldap yang dapat dimasukkan pada host infrastruktur untuk melihat informasi terkait konfigurasi AD. Domain dan parameter lain yang digunakan harus mencerminkan parameter yang dimasukkan pada waktu pembuatan lingkungan.

```
ldapsearch "(cn=AWS Delegated Add Workstations To Domain Users)" -x -h corp.res.com
-b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
-w <password>

ldapsearch "(&(objectClass=group))" -x -h corp.res.com
-b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
-w <password>
```

Debugging Windows DCV

Pada desktop Windows, Anda dapat membuat daftar sesi yang terkait dengannya menggunakan yang berikut ini:

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files\NICE\DCV\Server\bin\dcv.exe' list-sessions
Session: 'a7953489-9dbf-492b-8135-7709dccc4cab' (owner:admin2 type:console
name:windows1)
```

Temukan Informasi Versi Amazon DCV

Amazon DCV digunakan untuk sesi desktop virtual. [AWS Amazon DCV](#). Contoh berikut menunjukkan cara menentukan versi perangkat lunak DCV yang diinstal.

Linux

```
[root@ip-10-3-157-194 ~]# /usr/bin/dcv version

Amazon DCV 2023.0 (r14852)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Windows

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files\NICE\DCV\Server\bin\dcv.exe' version

Amazon DCV 2023.0 (r15065)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Masalah RunBooks

Bagian berikut berisi masalah yang mungkin terjadi, cara mendeteksinya, dan saran tentang cara mengatasi masalah tersebut.

- [Masalah instalasi](#)
 - [Saya ingin mengatur domain khusus setelah saya menginstal RES](#)
 - [AWS CloudFormation tumpukan gagal dibuat dengan pesan "WaitCondition menerima pesan gagal. Kesalahan:Negara. TaskFailed"](#)
 - [Pemberitahuan email tidak diterima setelah AWS CloudFormation tumpukan berhasil dibuat](#)
 - [Instance bersepeda atau vdc-controller dalam keadaan gagal](#)
 - [CloudFormation Tumpukan lingkungan gagal dihapus karena kesalahan objek dependen](#)
 - [Kesalahan ditemui untuk parameter blok CIDR selama pembuatan lingkungan](#)
 - [CloudFormation kegagalan pembuatan tumpukan selama pembuatan lingkungan](#)
 - [Pembuatan tumpukan sumber daya eksternal \(demo\) gagal dengan AdDomainAdminNode CREATE_FAILED](#)
- [Masalah manajemen identitas](#)
 - [Saya tidak berwenang untuk melakukan iam: PassRole](#)
 - [Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses Studio Penelitian dan Teknik saya tentang AWS sumber daya](#)
 - [Saat masuk ke lingkungan, saya segera kembali ke halaman login](#)
 - [Kesalahan "Pengguna tidak ditemukan" saat mencoba masuk](#)
 - [Pengguna ditambahkan di Active Directory, tetapi hilang dari RES](#)
 - [Pengguna tidak tersedia saat membuat sesi](#)
 - [Batas ukuran melebihi kesalahan dalam log CloudWatch pengelola kluster](#)
- [Penyimpanan](#)
 - [Saya membuat sistem file melalui RES tetapi tidak dipasang di host VDI](#)
 - [Saya memasukkan sistem file melalui RES tetapi tidak dipasang di host VDI](#)
 - [Saya tidak dapat mengaktifkan read/write dari host VDI](#)
 - [Contoh izin menangani kasus penggunaan](#)
 - [Saya membuat Amazon FSx untuk NetApp ONTAP dari RES tetapi tidak bergabung dengan domain saya](#)

- [Snapshot](#)
 - [Snapshot memiliki status Gagal](#)
 - [Snapshot gagal diterapkan dengan log yang menunjukkan bahwa tabel tidak dapat diimpor.](#)
- [Infrastruktur](#)
 - [Kelompok sasaran penyeimbang beban tanpa instance yang sehat](#)
- [Meluncurkan Desktop Virtual](#)
 - [Desktop virtual yang sebelumnya berfungsi tidak lagi dapat terhubung dengan sukses](#)
 - [Saya hanya dapat meluncurkan 5 desktop virtual](#)
 - [Upaya koneksi Windows Desktop gagal dengan “Koneksi telah ditutup. Kesalahan transportasi”](#)
 - [VDIs terjebak dalam status Penyediaan](#)
 - [VDIs masuk ke status Kesalahan setelah diluncurkan](#)
- [Komponen Desktop Virtual](#)
 - [EC2 Instans Amazon berulang kali ditampilkan dihentikan di konsol](#)
 - [instance vdc-controller sedang bersepeda karena gagal bergabung dengan modul AD/eVDI menunjukkan Pemeriksaan Kesehatan API Gagal](#)
 - [Proyek tidak muncul di pull down saat mengedit Software Stack untuk menambahkannya](#)
 - [pengelola klaster Log CloudWatch Amazon menunjukkan “user-home-init< > akun belum tersedia. menunggu pengguna untuk disinkronkan” \(di mana akun adalah nama pengguna\)](#)
 - [Desktop Windows pada upaya login mengatakan “Akun Anda telah dinonaktifkan. Silakan lihat administrator Anda”](#)
 - [Masalah Opsi DHCP dengan konfigurasi external/customer AD](#)
 - [Kesalahan Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING](#)
- [Penghapusan Env](#)
 - [res-xxx-cluster tumpuk dalam status “DELETE_FAILED” dan tidak dapat dihapus secara manual karena kesalahan “Peran tidak valid atau tidak dapat diasumsikan”](#)
 - [Mengumpulkan Log](#)
 - [Mengunduh VDI Logs](#)
 - [Mengunduh log dari EC2 instance Linux](#)
 - [Mengunduh log dari EC2 instance Windows](#)
 - [Mengumpulkan log ECS untuk kesalahan WaitCondition](#)
- [Lingkungan demo](#)

- [Kesalahan login lingkungan demo saat menangani permintaan otentikasi ke penyedia identitas](#)
- [Demo stack keycloak tidak berfungsi](#)

Masalah instalasi

Topik

- [Saya ingin mengatur domain khusus setelah saya menginstal RES](#)
- [AWS CloudFormation tumpukan gagal dibuat dengan pesan "WaitCondition menerima pesan gagal. Kesalahan:Negara. TaskFailed"](#)
- [Pemberitahuan email tidak diterima setelah AWS CloudFormation tumpukan berhasil dibuat](#)
- [Instance bersepeda atau vdc-controller dalam keadaan gagal](#)
- [CloudFormation Tumpukan lingkungan gagal dihapus karena kesalahan objek dependen](#)
- [Kesalahan ditemui untuk parameter blok CIDR selama pembuatan lingkungan](#)
- [CloudFormation kegagalan pembuatan tumpukan selama pembuatan lingkungan](#)
- [Pembuatan tumpukan sumber daya eksternal \(demo\) gagal dengan AdDomainAdminNode CREATE_FAILED](#)

.....

Saya ingin mengatur domain khusus setelah saya menginstal RES

Note

Prasyarat: Anda harus menyimpan Sertifikat dan PrivateKey konten dalam rahasia Secrets Manager sebelum melakukan langkah-langkah ini.

Tambahkan sertifikat ke klien web

1. Perbarui sertifikat yang dilampirkan ke pendengar penyeimbang beban external-alb:
 - a. Arahkan ke penyeimbang beban eksternal RES di AWS konsol di bawah> Load EC2Balancing> Load Balancers.
 - b. Cari penyeimbang beban yang mengikuti konvensi `<env-name>-external-alb` penamaan.

- c. Periksa pendengar yang terpasang pada penyeimbang beban.
 - d. Perbarui pendengar yang memiliki SSL/TLS sertifikat Default yang dilampirkan dengan detail sertifikat baru.
 - e. Simpan perubahan Anda.
2. Dalam tabel pengaturan cluster:
- a. Temukan tabel pengaturan cluster di DynamoDB -> Tabel -> `<env-name>.cluster-settings`
 - b. Pergi ke Jelajahi Item dan Filter berdasarkan Atribut — nama “kunci”, Ketik “string”, kondisi “berisi”, dan nilai “external_alb”.
 - c. Setel `cluster.load_balancers.external_alb.certificates.provided` ke Benar.
 - d. Perbarui
`nilaicluster.load_balancers.external_alb.certificates.custom_dns_name`.
 Ini adalah nama domain khusus untuk antarmuka pengguna web.
 - e. Perbarui
`nilaicluster.load_balancers.external_alb.certificates.acm_certificate_arn`.
 Ini adalah Nama Sumber Daya Amazon (ARN) untuk sertifikat terkait yang disimpan di Amazon Certificate Manager (ACM).
3. Perbarui catatan subdomain Route53 yang sesuai yang Anda buat untuk klien web Anda untuk menunjuk ke nama DNS penyeimbang beban alb eksternal. `<env-name>-external-alb`
4. Jika SSO sudah dikonfigurasi di lingkungan, konfigurasi ulang SSO dengan input yang sama seperti yang Anda gunakan pada awalnya dari Pengaturan Umum > Penyedia Identitas > Masuk Tunggal > Status > Edit tombol di portal web RES.

Tambahkan sertifikat ke VDIs

1. Berikan izin aplikasi RES untuk melakukan GetSecret operasi pada rahasia dengan menambahkan tag berikut ke rahasia:
 - `res:EnvironmentName : <env-name>`
 - `res:ModuleName : virtual-desktop-controller`
2. Dalam tabel pengaturan cluster:

- a. Temukan tabel pengaturan cluster di DynamoDB -> Tabel -> `<env-name>.cluster-settings`
 - b. Pergi ke Jelajahi Item dan Filter berdasarkan Atribut — nama “kunci”, Ketik “string”, kondisi “berisi”, dan nilai “dcv_connection_gateway”.
 - c. Setel `vdc.dcv_connection_gateway.certificate.provided` ke Benar.
 - d. Perbarui nilai `vdc.dcv_connection_gateway.certificate.custom_dns_name`. Ini adalah nama domain khusus untuk akses VDI.
 - e. Perbarui nilai `vdc.dcv_connection_gateway.certificate.certificate_secret_arn`. Ini adalah ARN untuk rahasia yang menyimpan isi Sertifikat.
 - f. Perbarui nilai `vdc.dcv_connection_gateway.certificate.private_key_secret_arn`. Ini adalah ARN untuk rahasia yang menyimpan isi Private Key.
3. Perbarui template peluncuran yang digunakan untuk instance gateway:
- a. Buka grup Auto Scaling di AWS Konsol di bawah> Auto Scaling EC2> Auto Scaling Groups.
 - b. Pilih grup penskalaan otomatis gateway yang sesuai dengan lingkungan RES. Nama mengikuti konvensi penamaan `<env-name>-vdc-gateway-asg`.
 - c. Temukan dan buka Template Peluncuran di bagian detail.
 - d. Di bawah Detail > Tindakan > pilih Ubah template (Buat versi baru).
 - e. Gulir ke bawah ke detail lanjutan.
 - f. Gulir ke bagian paling bawah, ke data Pengguna.
 - g. Carilah kata-katanya `CERTIFICATE_SECRET_ARN` dan `PRIVATE_KEY_SECRET_ARN`. Perbarui nilai-nilai ini dengan ARNs diberikan ke rahasia yang menyimpan konten Sertifikat (lihat langkah 2.c) dan Kunci Pribadi (lihat langkah 2.d).
 - h. Pastikan grup Auto Scaling dikonfigurasi untuk menggunakan versi template peluncuran yang baru dibuat (dari halaman grup Auto Scaling).
4. Perbarui catatan subdomain Route53 yang sesuai yang Anda buat untuk desktop virtual Anda untuk menunjuk ke nama DNS penyeimbang beban nlb eksternal: `<env-name>-external-nlb`
5. Hentikan instance `dcv-gateway` yang ada: `<env-name>-vdc-gateway` dan tunggu yang baru berputar.

.....

AWS CloudFormation tumpukan gagal dibuat dengan pesan "WaitCondition menerima pesan gagal. Kesalahan:Negara. TaskFailed"

Untuk mengidentifikasi masalah, periksa grup CloudWatch log Amazon bernama <stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>. Jika ada beberapa grup log dengan nama yang sama, periksa yang pertama tersedia. Pesan kesalahan dalam log akan memberikan informasi lebih lanjut tentang masalah ini.

 Note

Konfirmasikan bahwa nilai parameter tidak memiliki spasi.

.....

Pemberitahuan email tidak diterima setelah AWS CloudFormation tumpukan berhasil dibuat

Jika undangan email tidak diterima setelah AWS CloudFormation tumpukan berhasil dibuat, verifikasi hal berikut:

1. Konfirmasikan parameter alamat email dimasukkan dengan benar.

Jika alamat email salah atau tidak dapat diakses, hapus dan gunakan kembali lingkungan Studio Riset dan Teknik.

2. Periksa EC2 konsol Amazon untuk bukti kejadian bersepeda.

Jika ada EC2 instance Amazon dengan <envname> awalan yang muncul sebagai dihentikan dan kemudian diganti dengan instance baru, mungkin ada masalah dengan konfigurasi jaringan atau Direktori Aktif.

3. Jika Anda menerapkan resep Komputasi Kinerja AWS Tinggi untuk membuat sumber daya eksternal, konfirmasikan bahwa VPC, subnet pribadi dan publik, dan parameter lain yang dipilih dibuat oleh tumpukan.

Jika salah satu parameter salah, Anda mungkin perlu menghapus dan menerapkan kembali lingkungan RES. Untuk informasi selengkapnya, lihat [Copot pemasangan produk](#).

4. Jika Anda menerapkan produk dengan sumber daya eksternal Anda sendiri, konfirmasi jaringan dan Active Directory cocok dengan konfigurasi yang diharapkan.

Mengonfirmasi bahwa instance infrastruktur berhasil bergabung dengan Active Directory sangat penting. Coba langkah-langkah [the section called “Instance bersepeda atau vdc-controller dalam keadaan gagal”](#) untuk menyelesaikan masalah.

.....

Instance bersepeda atau vdc-controller dalam keadaan gagal

Penyebab paling mungkin dari masalah ini adalah ketidakmampuan sumber daya untuk menghubungkan atau bergabung dengan Active Directory.

Untuk memverifikasi masalah:

1. Dari baris perintah, mulailah sesi dengan SSM pada instance yang sedang berjalan dari vdc-controller.
2. Jalankan `sudo su -`.
3. Jalankan `systemctl status sssd`.

Jika status tidak aktif, gagal, atau Anda melihat kesalahan di log, maka instance tidak dapat bergabung dengan Active Directory.

Log kesalahan SSM

Untuk mengatasi masalah ini:

- Dari instance baris perintah yang sama, jalankan `cat /root/bootstrap/logs/userdata.log` untuk menyelidiki log.

Masalah ini bisa memiliki salah satu dari tiga kemungkinan akar penyebab.

Akar penyebab 1: Detail koneksi ldap salah dimasukkan

Tinjau log. Jika Anda melihat hal berikut diulang beberapa kali, instance tidak dapat bergabung dengan Active Directory.

```

+ local AD_AUTHORIZATION_ENTRY=
+ [[ -z '' ]]
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
34 seconds ...
+ sleep 34
+ (( ATTEMPT_COUNT++ ))

```

1. Verifikasi nilai parameter untuk yang berikut dimasukkan dengan benar selama pembuatan tumpukan RES.
 - directoryservice.ldap_connection_uri
 - directoryservice.ldap_base
 - directoryservice.users.ou
 - directoryservice.groups.ou
 - directoryservice.sudoers.ou
 - directoryservice.computers.ou
 - directoryservice.name
2. Perbarui nilai yang salah dalam tabel DynamoDB. Tabel ditemukan di konsol DynamoDB di bawah Tabel. Nama tabel harus **<stack name>.cluster-settings**.
3. Setelah Anda memperbarui tabel, hapus cluster-manager dan vdc-controller yang saat ini menjalankan instance lingkungan. Penskalaan otomatis akan memulai instance baru menggunakan nilai terbaru dari tabel DynamoDB.

Akar penyebab 2: ServiceAccount Nama pengguna salah dimasukkan

Jika log kembali `Insufficient permissions to modify computer account`, ServiceAccount nama yang dimasukkan selama pembuatan tumpukan bisa salah.

1. Dari AWS Konsol, buka Secrets Manager.
2. Cari `directoryserviceServiceAccountUsername`. Rahasiannya seharusnya **<stack name>-directoryservice-ServiceAccountUsername**.

3. Buka rahasia untuk melihat halaman detail. Di bawah Nilai Rahasia, pilih Ambil nilai rahasia dan pilih Plaintext.
4. Jika nilai diperbarui, hapus instance cluster-manager dan vdc-controller lingkungan yang sedang berjalan. Penskalaan otomatis akan memulai instance baru menggunakan nilai terbaru dari Secrets Manager.

Akar penyebab 3: ServiceAccount Kata sandi salah dimasukkan

Jika log ditampilkan `Invalid credentials`, ServiceAccount kata sandi yang dimasukkan selama pembuatan tumpukan mungkin salah.

1. Dari AWS Konsol, buka Secrets Manager.
2. Cari `directoryserviceServiceAccountPassword`. Rahasiannya seharusnya `<stack name>-directoryservice-ServiceAccountPassword`.
3. Buka rahasia untuk melihat halaman detail. Di bawah Nilai Rahasia, pilih Ambil nilai rahasia dan pilih Plaintext.
4. Jika Anda lupa kata sandi atau Anda tidak yakin apakah kata sandi yang dimasukkan benar, Anda dapat mengatur ulang kata sandi di Active Directory dan Secrets Manager.
 - a. Untuk mengatur ulang kata sandi di AWS Managed Microsoft AD:
 - i. Buka AWS konsol dan pergi ke AWS Directory Service.
 - ii. Pilih ID Direktori untuk direktori RES Anda, dan pilih Tindakan.
 - iii. Pilih Setel ulang kata sandi pengguna.
 - iv. Masukkan nama ServiceAccount pengguna.
 - v. Masukkan kata sandi baru, dan pilih Reset kata sandi.
 - b. Untuk mengatur ulang kata sandi di Secrets Manager:
 - i. Buka AWS konsol dan pergi ke Secrets Manager.
 - ii. Cari `directoryserviceServiceAccountPassword`. Rahasiannya seharusnya `<stack name>-directoryservice-ServiceAccountPassword`.
 - iii. Buka rahasia untuk melihat halaman detail. Di bawah Nilai Rahasia, pilih Ambil nilai rahasia lalu pilih Plaintext.
 - iv. Pilih Edit.
 - v. Tetapkan kata sandi baru untuk ServiceAccount pengguna dan pilih Simpan.

5. Jika Anda memperbarui nilainya, hapus instance cluster-manager dan vdc-controller lingkungan yang sedang berjalan. Penskalaan otomatis akan memulai instance baru menggunakan nilai terbaru.

.....

CloudFormation Tumpukan lingkungan gagal dihapus karena kesalahan objek dependen

Jika penghapusan `<env-name>-vdc` CloudFormation tumpukan gagal karena kesalahan objek dependen seperti `vdcvhostsecuritygroup`, ini bisa disebabkan oleh EC2 instance Amazon yang diluncurkan ke subnet atau grup keamanan yang dibuat RES menggunakan Konsol. AWS

Untuk mengatasi masalah ini, temukan dan hentikan semua EC2 instans Amazon yang diluncurkan dengan cara ini. Anda kemudian dapat melanjutkan penghapusan lingkungan.

.....

Kesalahan ditemui untuk parameter blok CIDR selama pembuatan lingkungan

Saat membuat lingkungan, kesalahan muncul untuk parameter blok CIDR dengan status respons [GAGAL].

Contoh kesalahan:

```
Failed to update cluster prefix list:
  An error occurred (InvalidParameterValue) when calling the
  ModifyManagedPrefixList operation:
    The specified CIDR (52.94.133.132/24) is not valid. For example, specify a CIDR
    in the following form: 10.0.0.0/16.
```

Untuk mengatasi masalah ini, format yang diharapkan adalah `x.x.x.0/24` atau `x.x.x.0/32`.

.....

CloudFormation kegagalan pembuatan tumpukan selama pembuatan lingkungan

Menciptakan lingkungan melibatkan serangkaian operasi pembuatan sumber daya. Di beberapa Wilayah, masalah kapasitas dapat terjadi yang menyebabkan pembuatan CloudFormation tumpukan gagal.

Jika ini terjadi, hapus lingkungan dan coba lagi pembuatannya. Atau, Anda dapat mencoba lagi pembuatan di Wilayah yang berbeda.

.....

Pembuatan tumpukan sumber daya eksternal (demo) gagal dengan AdDomainAdminNode CREATE_FAILED

Jika pembuatan tumpukan lingkungan demo gagal dengan kesalahan berikut, mungkin karena EC2 tambalan Amazon terjadi secara tak terduga selama penyediaan setelah peluncuran instance.

```
AdDomainAdminNode CREATE_FAILED Failed to receive 1 resource signal(s) within the specified duration
```

Untuk menentukan penyebab kegagalan:

1. Di SSM State Manager, periksa apakah patching dikonfigurasi dan apakah itu dikonfigurasi untuk semua instance.
2. Dalam riwayat RunCommand/Automation eksekusi SSM, periksa apakah eksekusi dokumen SSM terkait tambalan bertepatan dengan peluncuran instance.
3. Dalam file log untuk EC2 instans Amazon lingkungan, tinjau logging instans lokal untuk menentukan apakah instance di-boot ulang selama penyediaan.

Jika masalah disebabkan oleh patching, tunda patching untuk instans RES setidaknya 15 menit setelah peluncuran.

.....

Masalah manajemen identitas

Sebagian besar masalah dengan sistem masuk tunggal (SSO) dan manajemen identitas terjadi karena kesalahan konfigurasi. Untuk informasi tentang pengaturan konfigurasi SSO Anda, lihat:

- [the section called “Menyiapkan SSO dengan IAM Identity Center”](#)
- [the section called “Mengkonfigurasi penyedia identitas Anda untuk SSO”](#)

Untuk memecahkan masalah lain yang terkait dengan manajemen identitas, lihat topik pemecahan masalah berikut:

Topik

- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses Studio Penelitian dan Teknik saya tentang AWS sumber daya](#)
- [Saat masuk ke lingkungan, saya segera kembali ke halaman login](#)
- [Kesalahan “Pengguna tidak ditemukan” saat mencoba masuk](#)
- [Pengguna ditambahkan di Active Directory, tetapi hilang dari RES](#)
- [Pengguna tidak tersedia saat membuat sesi](#)
- [Batas ukuran melebihi kesalahan dalam log CloudWatch pengelola kluster](#)

.....

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan PassRole tindakan iam:, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke RES.

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

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

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

Dalam hal ini, kebijakan Mary harus diperbarui untuk memungkinkannya melakukan iam: PassRole action. Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

.....

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses Studio Penelitian dan Teknik saya tentang AWS sumber daya

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh AWS akun yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda ke AWS akun pihak ketiga, lihat [Menyediakan akses ke AWS akun yang dimiliki oleh pihak ketiga](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna yang diautentikasi secara eksternal \(federasi identitas\)](#) di Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, [lihat Perbedaan peran IAM dari kebijakan berbasis sumber daya di Panduan Pengguna IAM](#).

.....

Saat masuk ke lingkungan, saya segera kembali ke halaman login

Masalah ini terjadi ketika integrasi SSO Anda salah dikonfigurasi. Untuk menentukan masalah, periksa log instance pengontrol dan tinjau pengaturan konfigurasi untuk kesalahan.

Untuk memeriksa log:

1. Buka [konsol CloudWatch](#) .
2. Dari grup Log, temukan grup bernama `/<environment-name>/cluster-manager`.
3. Buka grup log untuk mencari kesalahan apa pun di aliran log.

Untuk memeriksa pengaturan konfigurasi:

1. Buka konsol [DynamoDB](#)
2. Dari Tabel, temukan tabel bernama `<environment-name>.cluster-settings`.
3. Buka tabel dan pilih Jelajahi item tabel.
4. Perluas bagian filter, dan masukkan variabel berikut:
 - Nama atribut - kunci
 - Kondisi - berisi
 - Nilai — sso
5. Pilih Jalankan.
6. Dalam string yang dikembalikan, verifikasi bahwa nilai konfigurasi SSO sudah benar. Jika salah, ubah nilai kunci `sso_enabled` menjadi `False`.
7. Kembali ke antarmuka pengguna RES untuk mengkonfigurasi ulang SSO.

.....

Kesalahan “Pengguna tidak ditemukan” saat mencoba masuk

Jika pengguna menerima kesalahan “Pengguna tidak ditemukan” ketika mereka mencoba masuk ke antarmuka RES, dan pengguna hadir di Active Directory:

- Jika pengguna tidak hadir di RES dan Anda baru saja menambahkan pengguna ke AD
 - Ada kemungkinan bahwa pengguna belum disinkronkan ke RES. RES disinkronkan setiap jam, jadi Anda mungkin perlu menunggu dan memeriksa apakah pengguna ditambahkan setelah sinkronisasi berikutnya. Untuk segera menyinkronkan, ikuti langkah-langkah [di Pengguna ditambahkan di Active Directory, tetapi hilang dari RES](#).
- Jika pengguna hadir di RES:
 1. Pastikan pemetaan atribut dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat [Mengkonfigurasi penyedia identitas Anda untuk single sign-on \(SSO\)](#).
 2. Pastikan bahwa subjek SAMP dan email SAMP keduanya dipetakan ke alamat email pengguna.

Pengguna ditambahkan di Active Directory, tetapi hilang dari RES

Note

Bagian ini berlaku untuk RES 2024.10 dan sebelumnya. Untuk RES 2024.12 dan yang lebih baru lihat. [Cara menjalankan sinkronisasi secara manual \(rilis 2024.12 dan yang lebih baru\)](#)

Jika Anda telah menambahkan pengguna ke Active Directory tetapi tidak ada di RES, sinkronisasi AD perlu dipicu. Sinkronisasi AD dilakukan setiap jam oleh fungsi Lambda yang mengimpor entri AD ke lingkungan RES. Terkadang, ada penundaan hingga proses sinkronisasi berikutnya berjalan setelah Anda menambahkan pengguna atau grup baru. Anda dapat memulai sinkronisasi secara manual dari Amazon Simple Queue Service.

Memulai proses sinkronisasi secara manual:

1. Buka [konsol Amazon SQS](#).
2. Dari Antrian, pilih. `<environment-name>-cluster-manager-tasks.fifo`
3. Pilih Kirim dan terima pesan.
4. Untuk isi Pesan, masukkan:


```
{ "name": "adsync.sync-from-ad", "payload": {} }
```
5. Untuk ID grup Pesan, masukkan: **adsync.sync-from-ad**
6. Untuk ID deduplikasi Pesan, masukkan string alfa-numerik acak. Entri ini harus berbeda dari semua panggilan yang dilakukan dalam lima menit sebelumnya atau permintaan akan diabaikan.

Pengguna tidak tersedia saat membuat sesi

Jika Anda seorang administrator yang membuat sesi, tetapi menemukan bahwa pengguna yang berada di Direktori Aktif tidak tersedia saat membuat sesi, pengguna mungkin perlu masuk untuk pertama kalinya. Sesi hanya dapat dibuat untuk pengguna aktif. Pengguna aktif harus masuk ke lingkungan setidaknya sekali.

Batas ukuran melebihi kesalahan dalam log CloudWatch pengelola klaster

```
2023-10-31T18:03:12.942-07:00 ldap.SIZELIMIT_EXCEEDED: {'msgtype': 100, 'msgid': 11, 'result': 4, 'desc': 'Size limit exceeded', 'ctrls': []}
```

Jika Anda menerima kesalahan ini di log CloudWatch pengelola klaster, pencarian ldap mungkin telah mengembalikan terlalu banyak catatan pengguna. Untuk memperbaiki masalah ini, tingkatkan batas hasil pencarian ldap IDP Anda.

.....

Penyimpanan

Topik

- [Saya membuat sistem file melalui RES tetapi tidak dipasang di host VDI](#)
- [Saya memasukkan sistem file melalui RES tetapi tidak dipasang di host VDI](#)
- [Saya tidak dapat mengaktifkan read/write dari host VDI](#)
- [Saya membuat Amazon FSx untuk NetApp ONTAP dari RES tetapi tidak bergabung dengan domain saya](#)

.....

Saya membuat sistem file melalui RES tetapi tidak dipasang di host VDI

Sistem file harus dalam keadaan “Tersedia” sebelum dapat dipasang oleh host VDI. Ikuti langkah-langkah di bawah ini untuk memvalidasi sistem file dalam keadaan wajib.

Amazon EFS

1. Buka [konsol Amazon EFS](#).
2. Periksa apakah status sistem File Tersedia.
3. Jika status sistem file tidak Tersedia, tunggu sebelum meluncurkan host VDI.

Amazon FSx ONTAP

1. Buka [FSx konsol Amazon](#).

2. Periksa apakah statusnya tersedia.
3. Jika Status tidak Tersedia, tunggu sebelum meluncurkan host VDI.

.....

Saya memasukkan sistem file melalui RES tetapi tidak dipasang di host VDI

Sistem file yang terpasang pada RES harus memiliki aturan grup keamanan yang diperlukan yang dikonfigurasi untuk memungkinkan host VDI memasang sistem file. Karena sistem file ini dibuat secara eksternal ke RES, RES tidak mengelola aturan grup keamanan terkait.

Grup keamanan yang terkait dengan sistem file onboard harus mengizinkan lalu lintas masuk berikut:

- Lalu lintas NFS (port: 2049) dari host VDC linux
- Lalu lintas SMB (port: 445) dari host windows VDC

.....

Saya tidak dapat mengaktifkan read/write dari host VDI

ONTAP mendukung UNIX, NTFS dan gaya keamanan MIXED untuk volume. Gaya keamanan menentukan jenis izin yang digunakan ONTAP untuk mengontrol akses data dan jenis klien apa yang dapat memodifikasi izin ini.

Misalnya, jika volume menggunakan gaya keamanan UNIX, klien SMB masih dapat mengakses data (asalkan mereka benar mengautentikasi dan mengotorisasi) karena sifat multi-protokol ONTAP. Namun, ONTAP menggunakan izin UNIX yang hanya dapat dimodifikasi oleh klien UNIX menggunakan alat asli.

Contoh izin menangani kasus penggunaan

Menggunakan volume gaya UNIX dengan beban kerja Linux

Izin dapat dikonfigurasi oleh sudoer untuk pengguna lain. Misalnya, berikut ini akan memberikan semua anggota read/write izin <group-ID> penuh pada /<project-name> direktori:

```
sudo chown root:<group-ID> /<project-name>
sudo chmod 770 /<project-name>
```

Menggunakan volume gaya NTFS dengan beban kerja Linux dan Windows

Izin Berbagi dapat dikonfigurasi menggunakan properti berbagi folder tertentu. Misalnya, diberikan pengguna `user_01` dan folder `myfolder`, Anda dapat mengatur izin `Full Control`, `Change`, atau `Read` ke `Allow` atau `Deny`:

Jika volume akan digunakan oleh klien Linux dan Windows, kita perlu mengatur pemetaan nama pada SVM yang akan mengaitkan nama pengguna Linux apa pun ke nama pengguna yang sama dengan format nama domain NetBIOS dari domain\username. Ini diperlukan untuk menerjemahkan antara pengguna Linux dan Windows. Untuk referensi, lihat [Mengaktifkan beban kerja multiprotokol dengan Amazon FSx](#) untuk ONTAP. NetApp

.....

Saya membuat Amazon FSx untuk NetApp ONTAP dari RES tetapi tidak bergabung dengan domain saya

Saat ini, saat Anda membuat Amazon FSx untuk NetApp ONTAP dari konsol RES, sistem file akan disediakan tetapi tidak bergabung dengan domain. Untuk menggabungkan SVM sistem file ONTAP yang dibuat ke domain Anda, lihat [Bergabung SVMs ke Microsoft Active Directory](#) dan ikuti langkah-langkah di konsol [Amazon FSx](#). Pastikan [izin yang diperlukan didelegasikan ke Akun FSx Layanan Amazon di AD](#). Setelah SVM berhasil bergabung dengan domain, buka Ringkasan SVM > Titik Akhir > nama DNS SMB, dan salin nama DNS karena Anda akan membutuhkannya nanti.

Setelah bergabung ke domain, edit kunci konfigurasi SMB DNS di tabel DynamoDB pengaturan cluster:

1. Buka konsol [Amazon DynamoDB](#).
2. Pilih Tabel, lalu pilih `<stack-name>-cluster-settings`.
3. Di bawah Jelajahi item tabel, perluas Filter, dan masukkan filter berikut:
 - Nama atribut - kunci
 - Kondisi - Sama dengan
 - Nilai - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. Pilih item yang dikembalikan, lalu Tindakan, Edit item.
5. Perbarui nilai dengan nama DNS SMB yang Anda salin sebelumnya.
6. Pilih Save and close (Simpan dan pilih).

Selain itu, pastikan grup keamanan yang terkait dengan sistem file memungkinkan lalu lintas seperti yang direkomendasikan dalam [Kontrol Akses Sistem File dengan Amazon VPC](#). Host VDI baru yang menggunakan sistem file sekarang akan dapat me-mount domain yang bergabung dengan SVM dan sistem file.

Atau, Anda dapat menggunakan sistem file yang sudah ada yang sudah bergabung ke domain Anda menggunakan kemampuan Sistem File Onboard RES- dari Manajemen Lingkungan pilih Sistem File, Sistem File Onboard.

Snapshot

Topik

- [Snapshot memiliki status Gagal](#)
- [Snapshot gagal diterapkan dengan log yang menunjukkan bahwa tabel tidak dapat diimpor.](#)

Snapshot memiliki status Gagal

Pada halaman RES Snapshots, jika snapshot memiliki status Gagal, penyebabnya dapat ditentukan dengan membuka grup CloudWatch log Amazon untuk pengelola klaster selama kesalahan terjadi.

```
[2023-11-19 03:39:20,208] [INFO] [snapshots-service] creating snapshot in S3 Bucket:
asdf at path s31
[2023-11-19 03:39:20,381] [ERROR] [snapshots-service] An error occurred while
creating the snapshot: An error occurred (TableNotFoundException)
when calling the UpdateContinuousBackups operation:
Table not found: res-demo.accounts.sequence-config
```

Snapshot gagal diterapkan dengan log yang menunjukkan bahwa tabel tidak dapat diimpor.

Jika snapshot yang diambil dari env sebelumnya gagal diterapkan di env baru, lihat CloudWatch log untuk pengelola klaster untuk mengidentifikasi masalah. Jika masalah menyebutkan bahwa cloud tabel yang diperlukan tidak diimpor, verifikasi bahwa snapshot dalam status valid.

1. Unduh file metadata.json dan verifikasi bahwa ExportStatus untuk berbagai tabel memiliki status SELESAI. Pastikan berbagai tabel memiliki ExportManifest bidang yang ditetapkan. Jika Anda tidak menemukan set bidang di atas, snapshot dalam keadaan tidak valid dan tidak dapat digunakan dengan fungsionalitas snapshot diterapkan.
2. Setelah memulai pembuatan snapshot, pastikan status Snapshot berubah menjadi SELESAI di RES. Proses pembuatan Snapshot memakan waktu hingga 5 hingga 10 menit. Muat ulang atau kunjungi kembali halaman Manajemen Snapshot untuk memastikan Snapshot berhasil dibuat. Ini akan memastikan bahwa snapshot yang dibuat dalam keadaan valid.

.....

Infrastruktur

Topik

- [Kelompok sasaran penyeimbang beban tanpa instance yang sehat](#)

.....

Kelompok sasaran penyeimbang beban tanpa instance yang sehat

Jika masalah seperti pesan kesalahan server muncul di UI atau sesi desktop tidak dapat terhubung, itu mungkin menunjukkan masalah dalam infrastruktur EC2 instans Amazon.

Metode untuk menentukan sumber masalah adalah dengan terlebih dahulu memeriksa EC2 konsol Amazon untuk setiap EC2 instance Amazon yang tampaknya berulang kali dihentikan dan digantikan oleh instance baru. Jika itu masalahnya, memeriksa CloudWatch log Amazon dapat menentukan penyebabnya.

Metode lain adalah memeriksa penyeimbang beban dalam sistem. Indikasi bahwa mungkin ada masalah sistem adalah jika ada penyeimbang beban, yang ditemukan di EC2 konsol Amazon, tidak menunjukkan instans sehat yang terdaftar.

Contoh penampilan normal ditunjukkan di sini:

Jika entri Sehat adalah 0, itu menunjukkan bahwa tidak ada EC2 instans Amazon yang tersedia untuk memproses permintaan.

Jika entri Tidak Sehat adalah non-0, itu menunjukkan bahwa EC2 instance Amazon mungkin bersepeda. Ini bisa disebabkan oleh perangkat lunak aplikasi yang diinstal tidak lulus pemeriksaan kesehatan.

Jika entri Sehat dan Tidak Sehat adalah 0, itu menunjukkan potensi kesalahan konfigurasi jaringan. Misalnya, subnet publik dan swasta mungkin tidak sesuai AZs. Jika kondisi ini terjadi, mungkin ada teks tambahan pada konsol yang menunjukkan bahwa status jaringan ada.

.....

Meluncurkan Desktop Virtual

Topik

- [Desktop virtual yang sebelumnya berfungsi tidak lagi dapat terhubung dengan sukses](#)
- [Saya hanya dapat meluncurkan 5 desktop virtual](#)
- [Upaya koneksi Windows Desktop gagal dengan “Koneksi telah ditutup. Kesalahan transportasi”](#)
- [VDIs terjebak dalam status Penyediaan](#)
- [VDIs masuk ke status Kesalahan setelah diluncurkan](#)

.....

Desktop virtual yang sebelumnya berfungsi tidak lagi dapat terhubung dengan sukses

Jika koneksi desktop ditutup atau Anda tidak dapat lagi terhubung dengannya, masalahnya mungkin disebabkan oleh kegagalan EC2 instans Amazon yang mendasarinya atau EC2 instans Amazon mungkin telah dihentikan atau dihentikan di luar lingkungan RES. Status UI Admin dapat terus menampilkan status siap tetapi upaya untuk menghubungkannya gagal.

EC2 Konsol Amazon harus digunakan untuk menentukan apakah instance telah dihentikan atau dihentikan. Jika berhenti, coba mulai lagi. Jika status dihentikan, desktop lain harus dibuat. Setiap data yang disimpan di direktori home pengguna harus tetap tersedia saat instance baru dimulai.

Jika instance yang gagal sebelumnya masih muncul di UI Admin, mungkin perlu dihentikan menggunakan UI Admin.

.....

Saya hanya dapat meluncurkan 5 desktop virtual

Batas default untuk jumlah desktop virtual yang dapat diluncurkan pengguna adalah 5. Ini dapat diubah oleh admin menggunakan UI Admin sebagai berikut:

- Buka Pengaturan Desktop.
- Pilih tab Server.
- Di panel Sesi DCV, klik ikon edit di sebelah kanan.
- Ubah nilai dalam Sesi yang Diizinkan Per Pengguna ke nilai baru yang diinginkan.
- Pilih Kirim.
- Segarkan halaman untuk mengonfirmasi bahwa pengaturan baru sudah ada.

.....

Upaya koneksi Windows Desktop gagal dengan “Koneksi telah ditutup. Kesalahan transportasi”

Jika koneksi desktop Windows gagal dengan kesalahan UI “Sambungan telah ditutup. Kesalahan transportasi”, penyebabnya dapat disebabkan oleh masalah dalam perangkat lunak server DCV yang terkait dengan pembuatan sertifikat pada instance Windows.

Grup CloudWatch log Amazon <envname>/vdc/dcv-connection-gateway dapat mencatat kesalahan upaya koneksi dengan pesan yang mirip dengan berikut ini:

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]
```

```
Nov 24 20:25:15.384 INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }
```

```
Nov 24 20:25:15.384 WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Error in websocket connection: Server unreachable: Server error: IO error:
```

```
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

Jika ini terjadi, resolusi mungkin menggunakan SSM Session Manager untuk membuka koneksi ke instance Windows dan menghapus 2 file terkait sertifikat berikut:

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv

Mode                LastWriteTime         Length Name
----                -
-a----            8/4/2022  12:59 PM         1704 dcv.key
-a----            8/4/2022  12:59 PM         1265 dcv.pem
```

File harus dibuat ulang secara otomatis dan upaya koneksi berikutnya mungkin berhasil.

Jika metode ini menyelesaikan masalah dan jika peluncuran baru desktop Windows menghasilkan kesalahan yang sama, gunakan fungsi Create Software Stack untuk membuat tumpukan perangkat lunak Windows baru dari instance tetap dengan file sertifikat yang dibuat ulang. Itu dapat menghasilkan tumpukan perangkat lunak Windows yang dapat digunakan untuk peluncuran dan koneksi yang sukses.

.....

VDIs terjebak dalam status Penyediaan

Jika peluncuran desktop tetap dalam status penyediaan di UI Admin, ini mungkin karena beberapa alasan.

Untuk menentukan penyebabnya, periksa file log pada instance desktop dan cari kesalahan yang mungkin menyebabkan masalah. Dokumen ini berisi daftar file log dan grup CloudWatch log Amazon yang berisi informasi yang relevan di bagian berlabel sumber informasi log dan peristiwa yang berguna.

Berikut ini adalah penyebab potensial dari masalah ini.

- Id AMI yang digunakan telah terdaftar sebagai tumpukan perangkat lunak tetapi tidak didukung oleh RES.

Skrip penyediaan bootstrap gagal diselesaikan karena Amazon Machine Image (AMI) tidak memiliki konfigurasi atau perkakas yang diharapkan. File log pada instance, seperti `/root/`

bootstrap/logs/ pada instance Linux, mungkin berisi informasi yang berguna mengenai hal ini. AMIs id yang diambil dari AWS Marketplace mungkin tidak berfungsi untuk instans desktop RES. Mereka memerlukan pengujian untuk mengkonfirmasi apakah mereka didukung.

- Skrip data pengguna tidak dijalankan ketika instance desktop virtual Windows diluncurkan dari AMI khusus.

Secara default, skrip data pengguna berjalan satu kali ketika EC2 instans Amazon diluncurkan. Jika Anda membuat AMI dari instance desktop virtual yang ada, maka daftarkan tumpukan perangkat lunak dengan AMI dan coba luncurkan desktop virtual lain dengan tumpukan perangkat lunak ini, skrip data pengguna tidak akan berjalan pada instance desktop virtual baru.

Untuk memperbaiki masalah, buka jendela PowerShell perintah sebagai Administrator pada instance desktop virtual asli yang Anda gunakan untuk membuat AMI, dan jalankan perintah berikut:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Kemudian buat AMI baru dari instance. Anda dapat menggunakan AMI baru untuk mendaftarkan tumpukan perangkat lunak dan meluncurkan desktop virtual baru setelahnya. Perhatikan bahwa Anda juga dapat menjalankan perintah yang sama pada instance yang tetap dalam status penyediaan dan me-reboot instance untuk memperbaiki sesi desktop virtual, tetapi Anda akan mengalami masalah yang sama lagi saat meluncurkan desktop virtual lain dari AMI yang salah konfigurasi.

.....

VDIs masuk ke status Kesalahan setelah diluncurkan

Kemungkinan masalah 1: Sistem file beranda memiliki direktori untuk pengguna dengan izin POSIX yang berbeda.

Ini bisa menjadi masalah yang Anda hadapi jika skenario berikut benar:

1. Versi RES yang digunakan adalah 2024.01 atau lebih tinggi.
2. Selama penerapan tumpukan RES, atribut untuk `EnableLdapIDMapping` disetel ke `True`.
3. Sistem file beranda yang ditentukan selama penerapan tumpukan RES digunakan dalam versi sebelum RES 2024.01 atau digunakan di lingkungan sebelumnya dengan disetel ke `EnableLdapIDMapping False`

Langkah resolusi: Hapus direktori pengguna di sistem file.

1. SSM ke host pengelola kluster.
2. `cd /home`.
3. `ls`- harus mencantumkan direktori dengan nama direktori yang cocok dengan nama pengguna, seperti `admin1`, `admin2`.. dan sebagainya.
4. Hapus direktori, `sudo rm -r 'dir_name'`. Jangan hapus direktori `ssm-user` dan `ec2-user`.
5. Jika pengguna sudah disinkronkan ke env baru, hapus pengguna dari tabel DDB pengguna (kecuali `clusteradmin`).
6. Memulai sinkronisasi AD - jalankan `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` di pengelola kluster Amazon. EC2
7. Reboot instance VDI di Error negara bagian dari halaman web RES. Validasi bahwa transisi VDI ke Ready status dalam waktu sekitar 20 menit.

.....

Komponen Desktop Virtual

Topik

- [EC2 Instans Amazon berulang kali ditampilkan dihentikan di konsol](#)
- [instance vdc-controller sedang bersepeda karena gagal bergabung dengan modul AD/eVDi menunjukkan Pemeriksaan Kesehatan API Gagal](#)
- [Proyek tidak muncul di pull down saat mengedit Software Stack untuk menambahkannya](#)
- [pengelola kluster Log CloudWatch Amazon menunjukkan “user-home-init< > akun belum tersedia. menunggu pengguna untuk disinkronkan” \(di mana akun adalah nama pengguna\)](#)
- [Desktop Windows pada upaya login mengatakan “Akun Anda telah dinonaktifkan. Silakan lihat administrator Anda”](#)
- [Masalah Opsi DHCP dengan konfigurasi external/customer AD](#)
- [Kesalahan Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING](#)

.....

EC2 Instans Amazon berulang kali ditampilkan dihentikan di konsol

Jika instance infrastruktur berulang kali ditampilkan sebagai dihentikan di EC2 konsol Amazon, penyebabnya mungkin terkait dengan konfigurasinya dan bergantung pada jenis instans infrastruktur. Berikut ini adalah metode untuk menentukan penyebabnya.

Jika instance vdc-controller menunjukkan status terminasi berulang di EC2 konsol Amazon, ini bisa disebabkan oleh tag Rahasia yang salah. Rahasia yang dikelola oleh RES memiliki tag yang digunakan sebagai bagian dari kebijakan kontrol akses IAM yang dilampirkan pada infrastruktur EC2 instans Amazon. Jika vdc-controller sedang bersepeda dan kesalahan berikut muncul di grup CloudWatch log, penyebabnya mungkin rahasia belum ditandai dengan benar. Perhatikan bahwa rahasia perlu ditandai dengan yang berikut:

```
{
  "res:EnvironmentName": "<envname>" # e.g. "res-demo"
  "res:ModuleName": "virtual-desktop-controller"
}
```

Pesan CloudWatch log Amazon untuk kesalahan ini akan muncul mirip dengan yang berikut:

```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

Periksa tag pada EC2 instance Amazon dan konfirmasikan bahwa mereka cocok dengan daftar di atas.

.....

instance vdc-controller sedang bersepeda karena gagal bergabung dengan modul AD/eVDi menunjukkan Pemeriksaan Kesehatan API Gagal

Jika modul eVDi gagal pemeriksaan kesehatannya, itu akan menampilkan yang berikut di bagian Status Lingkungan.

Dalam hal ini, jalur umum untuk debugging adalah dengan melihat log pengelola klaster. [CloudWatch](#) (Cari grup log bernama <env-name>/cluster-manager.)

Kemungkinan masalah:

- Jika log berisi teks `Insufficient permissions`, pastikan ServiceAccount nama pengguna yang diberikan saat tumpukan res dibuat dieja dengan benar.

Contoh baris log:

```
Insufficient permissions to modify computer account:
CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
000020E7: AttrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
(CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
request will be retried in 30 seconds
```

- Anda dapat mengakses ServiceAccount Nama Pengguna yang disediakan selama penerapan RES dari [SecretsManager konsol](#). Temukan rahasia yang sesuai di manajer Rahasia dan pilih Ambil teks Biasa. Jika Nama Pengguna salah, pilih Edit untuk memperbarui nilai rahasia. Hentikan instance cluster-manager dan vdc-controller saat ini. Contoh baru akan muncul dalam keadaan stabil.
- Nama pengguna harus "ServiceAccount" jika Anda memanfaatkan sumber daya yang dibuat oleh [tumpukan sumber daya eksternal](#) yang disediakan. Jika DisableADJoin parameter disetel ke False selama penyebaran RES Anda, pastikan pengguna "ServiceAccount" memiliki izin untuk membuat objek Komputer di AD.
- Jika nama pengguna yang digunakan benar, tetapi log berisi teks `Invalid credentials`, maka kata sandi yang Anda masukkan mungkin salah atau telah kedaluwarsa.

Contoh baris log:

```
{'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
data 532, v4563'}
```

- Anda dapat membaca kata sandi yang Anda masukkan selama pembuatan env dengan mengakses rahasia yang menyimpan kata sandi di konsol [Secrets Manager](#). Pilih rahasia (misalnya, <env_name>directoryserviceServiceAccountPassword) dan pilih Ambil teks biasa.

- Jika kata sandi dalam rahasia salah, pilih Edit untuk memperbarui nilainya dalam rahasia. Hentikan instance cluster-manager dan vdc-controller saat ini. Contoh baru akan menggunakan kata sandi yang diperbarui dan muncul dalam keadaan stabil.
- Jika kata sandi benar, bisa jadi kata sandi telah kedaluwarsa di Direktori Aktif yang terhubung. Anda harus terlebih dahulu mengatur ulang kata sandi di Active Directory dan kemudian memperbarui rahasianya. Anda dapat mengatur ulang kata sandi pengguna di Active Directory dari [konsol Directory Service](#):
 1. Pilih ID Direktori yang sesuai
 2. Pilih Tindakan, Setel ulang kata sandi pengguna lalu isi formulir dengan nama pengguna (misalnya, "ServiceAccount") dan kata sandi baru.
 3. Jika kata sandi yang baru ditetapkan berbeda dari kata sandi sebelumnya, perbarui kata sandi dalam rahasia Manajer Rahasia yang sesuai (misalnya, <env_name>directoryserviceServiceAccountPassword.
 4. Hentikan instance cluster-manager dan vdc-controller saat ini. Contoh baru akan muncul dalam keadaan stabil.

.....

Proyek tidak muncul di pull down saat mengedit Software Stack untuk menambahkannya

Masalah ini mungkin terkait dengan masalah berikut yang terkait dengan sinkronisasi akun pengguna dengan AD. Jika masalah ini muncul, periksa grup log CloudWatch Amazon pengelola klaster untuk kesalahan <user-home-init> account not available yet. waiting for user to be synced "" untuk menentukan apakah penyebabnya sama atau terkait.

.....

pengelola klaster Log CloudWatch Amazon menunjukkan “user-home-init< > akun belum tersedia. menunggu pengguna untuk disinkronkan” (di mana akun adalah nama pengguna)

Pelanggan SQS sibuk dan terjebak dalam loop tak terbatas karena tidak dapat masuk ke akun pengguna. Kode ini dipicu saat mencoba membuat sistem file beranda untuk pengguna selama sinkronisasi pengguna.

Alasan mengapa tidak dapat masuk ke akun pengguna mungkin karena RES tidak dikonfigurasi dengan benar untuk AD yang digunakan. Contohnya mungkin ServiceAccountCredentialsSecretArn parameter yang digunakan pada pembuatan BI/RES lingkungan bukanlah nilai yang benar.

.....

Desktop Windows pada upaya login mengatakan “Akun Anda telah dinonaktifkan. Silakan lihat administrator Anda”

Jika pengguna tidak dapat masuk kembali ke layar yang terkunci, ini mungkin menunjukkan bahwa pengguna telah dinonaktifkan di AD yang dikonfigurasi untuk RES setelah berhasil masuk melalui SSO.

Login SSO akan gagal jika akun pengguna telah dinonaktifkan di AD.

.....

Masalah Opsi DHCP dengan konfigurasi external/customer AD

Jika Anda menemukan kesalahan yang menyatakan "The connection has been closed. Transport error" dengan desktop virtual Windows saat menggunakan RES dengan Direktori Aktif Anda sendiri, periksa CloudWatch log dcv-connection-gateway Amazon untuk sesuatu yang mirip dengan yang berikut ini:

```
Oct 28 00:12:30.626 INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
lookup address information: Name or service not known" }

Oct 28 00:12:30.626 WARN HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
connection: Server unreachable: Server error: IO error: failed to lookup address
information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

Jika Anda menggunakan pengontrol domain AD untuk Opsi DHCP untuk VPC Anda sendiri, Anda perlu:

1. Tambahkan AmazonProvided DNS ke dua pengontrol IPs domain.
2. Atur nama domain ke ec2.internal.

Contoh ditampilkan di sini. Tanpa konfigurasi ini, desktop Windows akan memberi Anda kesalahan Transport, karena RES/DCV mencari nama host ip-10-0-x-xx.ec2.internal.

.....

Kesalahan Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Ketika Anda menggunakan browser web Firefox, Anda mungkin menemukan jenis pesan kesalahan MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING ketika Anda mencoba untuk terhubung ke desktop virtual.

Penyebabnya adalah server web RES diatur dengan TLS+Stapling On tetapi tidak merespons dengan Validasi Stapling (lihat <https://support.mozilla.org/en-US/questions/1372483>).

Anda dapat memperbaikinya dengan mengikuti petunjuk di: https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing.

.....

Penghapusan Env

Topik

- [res-xxx-cluster tumpuk dalam status “DELETE_FAILED” dan tidak dapat dihapus secara manual karena kesalahan “Peran tidak valid atau tidak dapat diasumsikan”](#)
- [Mengumpulkan Log](#)
- [Mengunduh VDI Logs](#)
- [Mengunduh log dari EC2 instance Linux](#)
- [Mengunduh log dari EC2 instance Windows](#)
- [Mengumpulkan log ECS untuk kesalahan WaitCondition](#)

.....

res-xxx-cluster tumpuk dalam status “DELETE_FAILED” dan tidak dapat dihapus secara manual karena kesalahan “Peran tidak valid atau tidak dapat diasumsikan”

Jika Anda melihat bahwa tumpukan "res-xxx-cluster" berada dalam status “DELETE_FAILED” dan tidak dapat dihapus secara manual, Anda dapat melakukan langkah-langkah berikut untuk menghapusnya.

Jika Anda melihat tumpukan dalam status “DELETE_FAILED”, pertama-tama coba hapus secara manual. Ini mungkin memunculkan dialog yang mengonfirmasi Hapus Tumpukan. Pilih Hapus.

Terkadang, bahkan jika Anda menghapus semua sumber daya tumpukan yang diperlukan, Anda mungkin masih melihat pesan untuk memilih sumber daya yang akan disimpan. Dalam hal ini, pilih semua sumber daya sebagai “sumber daya untuk dipertahankan” dan pilih Hapus.

Anda mungkin melihat kesalahan yang terlihat seperti `Role: arn:aws:iam:... is Invalid or cannot be assumed`

Ini berarti bahwa peran yang diperlukan untuk menghapus tumpukan dihapus terlebih dahulu sebelum tumpukan. Untuk menyiasatinya, salin nama perannya. Buka konsol IAM dan buat peran dengan nama itu menggunakan parameter seperti yang ditunjukkan di sini, yaitu:

- Untuk jenis entitas Tepercaya pilih AWS layanan.
- Untuk kasus Penggunaan, di bawah Use cases for other AWS services pilih CloudFormation.

Pilih Berikutnya. Pastikan Anda memberikan izin peran 'AWSCloudFormationFullAccess' dan AdministratorAccess ". Halaman ulasan Anda akan terlihat seperti ini:

Kemudian kembali ke CloudFormation konsol dan hapus tumpukan. Anda sekarang harus dapat menghapusnya sejak Anda membuat peran. Terakhir, buka konsol IAM dan hapus peran yang Anda buat.

.....

Mengumpulkan Log

Masuk ke EC2 instance dari EC2 konsol

- Ikuti [petunjuk ini](#) untuk masuk ke EC2 instans Linux Anda.
- Ikuti [petunjuk ini](#) untuk masuk ke EC2 instans Windows Anda. Kemudian buka Windows PowerShell untuk menjalankan perintah apa pun.

Mengumpulkan log host Infrastruktur

1. Cluster-manager: Dapatkan log untuk pengelola klaster dari tempat-tempat berikut dan lampirkan ke tiket.
 - a. Semua log dari grup CloudWatch log<env-name>/cluster-manager.
 - b. Semua log di bawah /root/bootstrap/logs direktori pada <env-name>-cluster-manager EC2 instance. Ikuti petunjuk yang ditautkan dari “Masuk ke EC2 instance dari EC2 konsol” di awal bagian ini untuk masuk ke instans Anda.
2. VDC-controller: Dapatkan log untuk vdc-controller dari tempat-tempat berikut dan lampirkan ke tiket.
 - a. Semua log dari grup CloudWatch log<env-name>/vdc-controller.
 - b. Semua log di bawah /root/bootstrap/logs direktori pada <env-name>-vdc-controller EC2 instance. Ikuti petunjuk yang ditautkan dari “Masuk ke EC2 instance dari EC2 konsol” di awal bagian ini untuk masuk ke instans Anda.

Salah satu cara untuk mendapatkan log dengan mudah adalah dengan mengikuti instruksi di [Mengunduh log dari EC2 instance Linux](#) bagian. Nama modul akan menjadi nama instance.

Mengumpulkan log VDI

Identifikasi EC2 instans Amazon yang sesuai

Jika pengguna meluncurkan VDI dengan nama sesiVDI1, nama instance yang sesuai di EC2 konsol Amazon adalah. <env-name>-VDI1-<user name>

Kumpulkan log VDI Linux

Masuk ke EC2 instans Amazon yang sesuai dari EC2 konsol Amazon dengan mengikuti instruksi yang ditautkan ke “Masuk ke EC2 instance dari EC2 konsol” di awal bagian ini. Dapatkan semua

log di bawah `/var/log/dcv/` direktori `/root/bootstrap/logs` dan pada instance VDI Amazon EC2 .

Salah satu cara untuk mendapatkan log adalah dengan mengunggahnya ke s3 dan kemudian mengunduhnya dari sana. Untuk itu, Anda dapat mengikuti langkah-langkah ini untuk mendapatkan semua log dari satu direktori dan kemudian mengunggahnya:

1. Ikuti langkah-langkah ini untuk menyalin log dcv di bawah `/root/bootstrap/logs` direktori:

```
sudo su -  
cd /root/bootstrap  
mkdir -p logs/dcv_logs  
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. Sekarang, ikuti langkah-langkah yang tercantum di bagian berikutnya- [Mengunduh VDI Logs](#) untuk mengunduh log.

Kumpulkan log Windows VDI

Masuk ke EC2 instans Amazon yang sesuai dari EC2 konsol Amazon dengan mengikuti instruksi yang ditautkan ke “Masuk ke EC2 instance dari EC2 konsol” di awal bagian ini. Dapatkan semua log di bawah `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` direktori pada EC2 instance VDI.

Salah satu cara untuk mendapatkan log adalah dengan mengunggahnya ke S3 dan kemudian mengunduhnya dari sana. Untuk melakukan itu, ikuti langkah-langkah yang tercantum di bagian berikutnya-[Mengunduh VDI Logs](#).

.....

Mengunduh VDI Logs

1. Perbarui peran IAM EC2 instance VDI untuk memungkinkan akses S3.
2. Buka EC2 konsol dan pilih instance VDI Anda.
3. Pilih peran IAM yang digunakannya.
4. Di bagian Kebijakan Izin dari menu tarik-turun Tambahkan izin, pilih Lampirkan Kebijakan lalu pilih kebijakan AmazonS3. FullAccess
5. Pilih Tambahkan izin untuk melampirkan kebijakan tersebut.
6. Setelah itu, ikuti langkah-langkah yang tercantum di bawah ini berdasarkan jenis VDI Anda untuk mengunduh log. Nama modul akan menjadi nama instance.

- a. [Mengunduh log dari EC2 instance Linux](#) untuk Linux.
 - b. [Mengunduh log dari EC2 instance Windows](#) untuk Windows.
7. Terakhir, edit peran untuk menghapus AmazonS3FullAccess kebijakan.

Note

Semua VDI menggunakan peran IAM yang sama yaitu `<env-name>-vdc-host-role-<region>`

Mengunduh log dari EC2 instance Linux

Masuk ke EC2 instance tempat Anda ingin mengunduh log dan jalankan perintah berikut untuk mengunggah semua log ke bucket s3:

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/${MODULE}_logs.tar.gz
```

Setelah ini, buka konsol S3, pilih ember dengan nama `<environment_name>-cluster-<region>-<aws_account_number>` dan unduh file yang diunggah `<module_name>_logs.tar.gz` sebelumnya.

Mengunduh log dari EC2 instance Windows

Masuk ke EC2 instance tempat Anda ingin mengunduh log dan jalankan perintah berikut untuk mengunggah semua log ke bucket S3:

```

$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath

```

Setelah ini, buka konsol S3, pilih ember dengan nama **<environment_name>-cluster-<region>-<aws_account_number>** dan unduh file yang diunggah **<module_name>_logs.zip** sebelumnya.

.....

Mengumpulkan log ECS untuk kesalahan WaitCondition

1. Buka tumpukan yang digunakan dan pilih tab Sumber Daya.
2. Perluas Deploy → ResearchAndEngineeringStudio → Installer → Tasks → CreateTaskDef → CreateContainer → LogGroup, dan pilih grup log untuk membuka CloudWatch log.
3. Ambil log terbaru dari grup log ini.

.....

Lingkungan demo

Topik

- [Kesalahan login lingkungan demo saat menangani permintaan otentikasi ke penyedia identitas](#)
- [Demo stack keycloak tidak berfungsi](#)

.....

Kesalahan login lingkungan demo saat menangani permintaan otentikasi ke penyedia identitas

Masalah

Jika Anda mencoba masuk dan mendapatkan 'Kesalahan tak terduga saat menangani permintaan otentikasi ke penyedia identitas', kata sandi Anda mungkin kedaluwarsa. Ini bisa berupa kata sandi untuk pengguna yang Anda coba masuk sebagai atau Active Directory Service Account Anda.

Mitigasi

1. Setel ulang kata sandi akun pengguna dan layanan di [konsol layanan direktori](#).
2. Perbarui kata sandi Akun Layanan di [Secrets Manager](#) agar sesuai dengan kata sandi baru yang Anda masukkan di atas:
 - untuk tumpukan Keycloak: PasswordSecret-... - RESExternal-... - DirectoryService-... dengan Deskripsi: Kata Sandi untuk Microsoft Active Directory
 - untuk RES: res- ServiceAccountPassword -... dengan Deskripsi: Active Directory Service Account Password
3. Buka [EC2 konsol](#) dan hentikan instance cluster-manager. Aturan Auto Scaling akan secara otomatis memicu penerapan instance baru.

.....

Demo stack keycloak tidak berfungsi

Masalah

Jika server keycloak Anda mogok dan, ketika Anda memulai ulang server, IP instance berubah, ini mungkin mengakibatkan kerusakan keycloak— halaman login portal RES Anda gagal memuat atau macet dalam status pemuatan yang tidak pernah diselesaikan.

Mitigasi

Anda harus menghapus infrastruktur yang ada dan menerapkan kembali tumpukan Keycloak untuk mengembalikan Keycloak ke keadaan sehat. Ikuti langkah-langkah ini:

1. Pergi ke Cloudformation. Anda akan melihat dua tumpukan terkait keycloak di sana:
 - *<env-name>-RESSsoKeycloak-<random characters>*(Tumpukan1)

`<env-name>-RESSsoKeycloak-<random characters>-RESSsoKeycloak-
*(Tumpukan2)`

2. Hapus Stack1. Jika diminta untuk menghapus tumpukan bersarang, pilih Ya untuk menghapus tumpukan bersarang.

Pastikan tumpukan telah dihapus sepenuhnya.

3. [Unduh template tumpukan Keycloak RES SSO di sini.](#)
4. Terapkan tumpukan ini secara manual dengan nilai parameter yang sama persis dengan tumpukan yang dihapus. Menyebarkannya dari CloudFormation konsol dengan pergi ke Create Stack → Dengan sumber daya baru (standar) → Pilih template yang ada → Upload file template. Isi parameter yang diperlukan menggunakan input yang sama dengan tumpukan yang dihapus. Anda dapat menemukan input ini di tumpukan yang dihapus dengan mengubah filter di CloudFormation konsol dan pergi ke tab Parameter. Pastikan bahwa nama lingkungan, key pair, dan parameter lainnya cocok dengan parameter stack asli.
5. Setelah tumpukan dikerahkan, lingkungan Anda siap digunakan lagi. Anda dapat menemukan ApplicationUrl di tab Output dari tumpukan yang digunakan.

.....

Masalah yang Diketahui

- [Masalah yang Diketahui 2024.x](#)
 - [\(2024.08\) Desktop virtual gagal memasang bucket Amazon S3 read/write dengan root bucket ARN dan awalan khusus](#)
 - [\(2024.06\) Menerapkan snapshot gagal saat nama grup AD berisi spasi](#)
 - [\(2024.04-2024.04.02\) Memberikan Batas Izin IAM yang tidak dilampirkan ke peran instans VDI](#)
 - [\(2024.04.02 dan sebelumnya\) Instans Windows NVIDIA di ap-southeast-2 \(Sydney\) gagal diluncurkan](#)
 - [\(2024.04 dan 2024.04.01\) Kegagalan penghapusan RES di GovCloud](#)
 - [\(2024.04 - 2024.04.02\) Desktop virtual Linux mungkin macet dalam status “MELANJUTKAN” saat reboot](#)
 - [\(2024.04.02 dan sebelumnya\) Gagal menyinkronkan pengguna AD yang atribut SAMAccount Namanya menyertakan huruf kapital atau karakter khusus](#)

- [\(2024.04.02 dan sebelumnya\) Kunci pribadi untuk mengakses host bastion tidak valid](#)
- [\(2024.06 dan sebelumnya\) Anggota grup tidak disinkronkan ke RES selama sinkronisasi AD](#)
- [\(2024.06 dan sebelumnya\) CVE-2024-6387, Regre, Kerentanan Keamanan di dan Ubuntu SSHion RHEL9 VDIs](#)

Masalah yang Diketahui 2024.x

.....

(2024.08) Desktop virtual gagal memasang bucket Amazon S3 read/write dengan root bucket ARN dan awalan khusus

Deskripsi bug

Research and Engineering Studio 2024.08 gagal memasang bucket read/write S3 ke instance infrastruktur desktop virtual (VDI) saat menggunakan bucket root ARN (yaitu, `arn:aws:s3:::example-bucket`) dan awalan khusus (nama proyek atau nama proyek dan nama pengguna).

Konfigurasi bucket yang tidak terpengaruh oleh masalah ini meliputi:

- ember hanya-baca
- baca/tulis bucket dengan awalan sebagai bagian dari bucket ARN (yaitu, `arn:aws:s3:::example-bucket/example-folder-prefix`) dan awalan kustom (nama proyek atau nama proyek dan nama pengguna)
- baca/tulis bucket dengan root bucket ARN, tetapi tidak ada awalan khusus

Setelah Anda menyediakan instance VDI, direktori mount yang ditentukan untuk bucket S3 tersebut tidak akan memiliki bucket yang terpasang. Meskipun direktori mount pada VDI akan ada, direktori akan kosong dan tidak akan berisi konten bucket saat ini. Saat Anda menulis file ke direktori menggunakan terminal, kesalahan `Permission denied, unable to write a file` akan dilemparkan dan konten file tidak akan diunggah ke ember S3 yang sesuai.

Versi yang terpengaruh

2024.08

Mitigasi

1. Untuk mengunduh skrip patch dan file patch (patch.pydans3_mount_custom_prefix_fix.patch), jalankan perintah berikut, ganti <output-directory> dengan direktori tempat Anda ingin mengunduh skrip patch dan file patch dan <environment-name> dengan nama lingkungan RES Anda:
 - a. Patch hanya berlaku untuk RES 2024.08.
 - b. [Skrip patch membutuhkan AWS CLI v2, Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
 - c. Konfigurasi AWS CLI untuk akun dan wilayah tempat RES diterapkan, dan pastikan Anda memiliki izin Amazon S3 untuk menulis ke bucket yang dibuat oleh RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

2. Arahkan ke direktori tempat skrip patch dan file patch diunduh. Jalankan perintah patch berikut:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. Untuk mengakhiri instance Virtual Desktop Controller (vdc-controller) untuk lingkungan Anda, jalankan perintah berikut. (Anda sudah mengatur ENVIRONMENT_NAME variabel ke nama lingkungan RES Anda di langkah pertama.)

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

Note

Untuk pengaturan VPC pribadi, jika Anda belum melakukannya, untuk `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda` fungsi pastikan untuk menambahkan Environment variable dengan nama `AWS_STS_REGIONAL_ENDPOINTS` dan nilai `regional`. Untuk informasi selengkapnya, lihat [Prasyarat bucket Amazon S3 untuk penerapan VPC yang terisolasi](#).

- Setelah grup target yang dimulai dengan nama `<RES-EnvironmentName>-vdc-ext` menjadi sehat, new perlu diluncurkan yang VDI akan memiliki bucket read/write S3 dengan root bucket ARN dan awalan khusus dipasang dengan benar.

.....

(2024.06) Menerapkan snapshot gagal saat nama grup AD berisi spasi

Masalah

RES 2024.06 gagal menerapkan snapshot dari versi sebelumnya jika grup AD berisi spasi dalam namanya.

CloudWatch Log pengelola klaster (di bawah grup `<environment-name>/cluster-manager log`) akan menyertakan kesalahan berikut selama sinkronisasi AD:

```
[apply-snapshot] authz.role-assignments/<Group name with spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key doesn't match the regex pattern ^[a-zA-Z0-9_.-]{1,20}: (user|group)$
```

Kesalahan hasil dari RES hanya menerima nama grup yang memenuhi persyaratan berikut:

- Ini hanya dapat berisi huruf kecil dan huruf besar ASCII, digit, tanda hubung (-), periode (.), dan garis bawah (_)
- Tanda hubung (-) tidak diperbolehkan sebagai karakter pertama
- Tidak dapat berisi spasi.

Versi yang terpengaruh

2024.06

Mitigasi

1. Untuk mengunduh skrip patch dan file patch ([patch.py](#) dan [groupname_regex.patch](#)), jalankan perintah berikut, ganti `<output-directory>` dengan direktori tempat Anda ingin meletakkan file, dan `<environment-name>` dengan nama lingkungan RES Anda:
 - a. Patch hanya berlaku untuk RES 2024.06
 - b. [Skrip patch membutuhkan AWS CLI v2, Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
 - c. Konfigurasi AWS CLI untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin S3 untuk menulis ke bucket yang dibuat oleh RES:

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. Arahkan ke direktori tempat skrip patch dan file patch diunduh. Jalankan perintah patch berikut:

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. Untuk memulai ulang instance Cluster Manager untuk lingkungan Anda, jalankan perintah berikut: Anda juga dapat menghentikan instance dari Amazon EC2 Management Console.

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

Note

Patch memungkinkan nama grup AD berisi huruf ASCII huruf kecil dan huruf besar ASCII, digit, tanda hubung (-), periode (.), garis bawah (_), dan spasi dengan panjang total antara 1 dan 30, inklusif.

.....

(2024.04-2024.04.02) Memberikan Batas Izin IAM yang tidak dilampirkan ke peran instans VDI

Masalah

Sesi desktop virtual tidak mewarisi konfigurasi batas izin proyek mereka dengan benar. Ini adalah hasil dari batas izin yang ditentukan oleh parameter IAMPermission Batas yang tidak ditetapkan dengan benar ke proyek selama pembuatan proyek tersebut.

Versi yang terpengaruh

2024.04 - 2024.04.02

Mitigasi

Ikuti langkah-langkah ini VDI untuk memungkinkan mewarisi batas izin yang ditetapkan ke proyek dengan benar:

1. Untuk mengunduh skrip patch dan file patch ([patch.py](#) dan [vdi_host_role_permission_boundary.patch](#)), jalankan perintah berikut, ganti dengan direktori lokal tempat Anda ingin meletakkan file: `<output-directory>`
 - a. Patch hanya berlaku untuk RES 2024.04.02. Jika Anda menggunakan versi 2024.04 atau 2024.04.01, Anda dapat mengikuti [langkah-langkah yang tercantum dalam dokumen publik untuk pembaruan versi minor untuk](#) memperbarui lingkungan Anda ke 2024.04.02.
 - b. [Skrip patch membutuhkan AWS CLI v2\), Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
 - c. Konfigurasi AWS CLI untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin S3 untuk menulis ke bucket yang dibuat oleh RES.

```
OUTPUT_DIRECTORY=<output-directory>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
--output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. Arahkan ke direktori tempat skrip patch dan file patch diunduh. Jalankan perintah patch berikut, ganti <environment-name> dengan nama lingkungan RES Anda:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. Mulai ulang instance pengelola kluster di lingkungan Anda dengan menjalankan perintah ini, ganti <environment-name> dengan nama lingkungan RES Anda. Anda juga dapat menghentikan instance dari Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 dan sebelumnya) Instans Windows NVIDIA di ap-southeast-2 (Sydney) gagal diluncurkan

Masalah

Amazon Machine Images (AMIs) digunakan untuk memutar virtual desktop (VDIs) di RES dengan konfigurasi tertentu. Setiap AMI memiliki ID terkait yang berbeda per wilayah. ID AMI yang dikonfigurasi dalam RES untuk meluncurkan instance Windows Nvidia di ap-southeast-2 (Sydney) saat ini salah.

AMI-ID `ami-0e190f8939a996caf` untuk jenis konfigurasi instans ini salah tercantum di `ap-southeast-2` (Sydney). ID AMI `ami-027cf6e71e2e442f4` harus digunakan sebagai gantinya.

Pengguna akan mendapatkan kesalahan berikut saat mencoba meluncurkan instance dengan `ami-0e190f8939a996caf` AMI default.

```
An error occurred (InvalidAMIID.NotFound) when calling the RunInstances operation: The image id '[ami-0e190f8939a996caf]' does not exist
```

Langkah-langkah untuk mereproduksi bug, termasuk contoh file konfigurasi:

- Menyebarkan RES di wilayah `ap-southeast-2`.
- Luncurkan instance menggunakan tumpukan perangkat lunak default Windows-NVIDIA (ID `ami-0e190f8939a996caf` AMI).

Versi yang terpengaruh

Semua versi RES 2024.04.02 atau sebelumnya terpengaruh

Mitigasi

Mitigasi berikut telah diuji pada RES versi 2024.01.01:

- Daftarkan tumpukan perangkat lunak baru dengan pengaturan berikut
 - ID AMI: `ami-027cf6e71e2e442f4`
 - Sistem Operasi: Windows
 - Produsen GPU: NVIDIA
 - Min. Ukuran Penyimpanan (GB): 30
 - Min. RAM (GB): 4
- Gunakan tumpukan perangkat lunak ini untuk meluncurkan instance Windows-NVIDIA

.....

(2024.04 dan 2024.04.01) Kegagalan penghapusan RES di GovCloud

Masalah

Selama alur kerja penghapusan RES, UnprotectCognitoUserPool Lambda menonaktifkan Perlindungan Penghapusan untuk Kumpulan Pengguna Cognito yang nantinya akan dihapus. Eksekusi Lambda dimulai oleh. InstallerStateMachine

Karena perbedaan versi AWS CLI default antara Komersil dan GovCloud wilayah, update_user_pool panggilan di Lambda akan gagal di wilayah. GovCloud

Pelanggan akan mendapatkan kesalahan berikut saat mencoba menghapus RES di GovCloud wilayah:

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection\n\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,\nSmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,\nVerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,\nDeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,\nAdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

Langkah-langkah untuk mereproduksi bug:

- Menyebarkan RES di suatu wilayah GovCloud
- Hapus tumpukan RES

Versi yang terpengaruh

RES versi 2024.04 dan 2024.04.01

Mitigasi

Mitigasi berikut telah diuji pada RES versi 2024.04:

- Buka UnprotectCognitoUserPool Lambda
 - Konvensi penamaan: **<env-name>-InstallerTasksUnprotectCognitoUserPool-...**
- Pengaturan Runtime -> Edit -> Pilih Runtime **Python 3.11** -> Simpan.
- Terbuka CloudFormation.
- Hapus tumpukan RES -> biarkan Retain Installer Resource TIDAK DICENTANG -> Hapus.

.....

(2024.04 - 2024.04.02) Desktop virtual Linux mungkin macet dalam status “MELANJUTKAN” saat reboot

Masalah

Desktop virtual Linux dapat terjebak dalam status “MELANJUTKAN” saat memulai ulang setelah pemberhentian manual atau terjadwal.

Setelah instance di-boot ulang, AWS Systems Manager tidak menjalankan perintah jarak jauh apa pun untuk membuat sesi DCV baru dan pesan log berikut hilang di log vdc-controller (di bawah grup CloudWatch log): <environment-name>/vdc/controller CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

Versi yang terpengaruh

2024.04 - 2024.04.02

Mitigasi

Untuk memulihkan desktop virtual yang terjebak dalam status “MELANJUTKAN”:

1. SSH ke dalam instance masalah dari EC2 konsol.
2. Jalankan perintah berikut pada instance:

```
sudo su -  
/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/  
configure_post_reboot.sh  
sudo reboot
```

3. Tunggu instance untuk reboot.

Untuk mencegah desktop virtual baru mengalami masalah yang sama:

1. Untuk mengunduh skrip patch dan file patch ([patch.py](#) dan [vdi_stuck_in_resuming_status.patch](#)), jalankan perintah berikut, ganti dengan direktori tempat Anda ingin meletakkan file: <output-directory>

 Note

- Patch hanya berlaku untuk RES 2024.04.02.
- [Scrip patch membutuhkan AWS CLI v2, Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
- Konfigurasi AWS CLI untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin S3 untuk menulis ke bucket yang dibuat oleh RES.

```
OUTPUT_DIRECTORY=<output-directory>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. Arahkan ke direktori tempat scrip patch dan file patch diunduh. Jalankan perintah patch berikut, ganti <environment-name> dengan nama lingkungan RES Anda dan <aws-region> dengan wilayah tempat RES digunakan:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
--module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. Untuk memulai ulang instance VDC Controller untuk lingkungan Anda, jalankan perintah berikut, ganti <environment-name> dengan nama lingkungan RES Anda:

```
ENVIRONMENT_NAME=<environment-name>
```

```
INSTANCE_ID=$(aws ec2 describe-instances \
--filters \
Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
--query "Reservations[0].Instances[0].InstanceId" \
--output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 dan sebelumnya) Gagal menyinkronkan pengguna AD yang atribut SAMAccount Namanya menyertakan huruf kapital atau karakter khusus

Masalah

RES gagal menyinkronkan pengguna AD setelah SSO diatur setidaknya selama dua jam (dua siklus sinkronisasi AD). CloudWatch Log pengelola kluster (di bawah grup <environment-name>/cluster-manager log) menyertakan kesalahan berikut selama sinkronisasi AD:

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

Kesalahan hasil dari RES hanya menerima SAMAccount nama pengguna yang memenuhi persyaratan berikut:

- Itu hanya dapat berisi huruf ASCII kecil, digit, periode (.), garis bawah (_).
- Periode atau garis bawah tidak diperbolehkan sebagai karakter pertama atau terakhir.
- Itu tidak dapat berisi dua periode berkesinambungan atau garis bawah (misalnya., __, ._, _.).

Versi yang terpengaruh

2024.04.02 dan sebelumnya

Mitigasi

1. Untuk mengunduh skrip patch dan file patch ([patch.py](#) dan [samaccountname_regex.patch](#)), jalankan perintah berikut, ganti <output-directory> dengan direktori tempat Anda ingin meletakkan file:

Note

- Patch hanya berlaku untuk RES 2024.04.02.
- [Skrip patch membutuhkan AWS CLI v2, Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
- Konfigurasi AWS CLI untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin S3 untuk menulis ke bucket yang dibuat oleh RES.

```
OUTPUT_DIRECTORY=<output-directory>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
${OUTPUT_DIRECTORY}/samaccountname_regex.patch
```

2. Arahkan ke direktori tempat skrip patch dan file patch diunduh. Jalankan perintah patch berikut, ganti <environment-name> dengan nama lingkungan RES Anda:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. Untuk memulai ulang instance Cluster Manager untuk lingkungan Anda, jalankan perintah berikut, ganti <environment-name> dengan nama lingkungan RES Anda. Anda juga dapat menghentikan instance dari Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>
```

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 dan sebelumnya) Kunci pribadi untuk mengakses host bastion tidak valid

Masalah

Ketika pengguna mengunduh kunci pribadi untuk mengakses host bastion dari portal web RES, kuncinya tidak diformat dengan baik — beberapa baris diunduh sebagai satu baris, yang membuat

kunci tidak valid. Pengguna akan mendapatkan kesalahan berikut ketika mereka mencoba mengakses host bastion dengan kunci yang diunduh:

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic)
```

Versi yang terpengaruh

2024.04.02 dan sebelumnya

Mitigasi

Kami merekomendasikan menggunakan Chrome untuk mengunduh kunci, karena browser ini tidak terpengaruh.

Atau, file kunci dapat diformat ulang dengan membuat baris baru setelah -----BEGIN PRIVATE KEY----- dan baris baru lainnya sebelumnya. -----END PRIVATE KEY-----

.....

(2024.06 dan sebelumnya) Anggota grup tidak disinkronkan ke RES selama sinkronisasi AD

Deskripsi bug

Anggota grup tidak akan melakukan sinkronisasi dengan benar ke RES jika GrouPou berbeda dari UseRou.

RES membuat filter ldapsearch saat mencoba menyinkronkan pengguna dari grup AD. Filter saat ini salah menggunakan parameter UseRou alih-alih parameter GrouPou. Hasilnya adalah pencarian gagal mengembalikan pengguna mana pun. Perilaku ini hanya terjadi dalam kasus di mana userSou dan GrouPou berbeda.

Versi yang terpengaruh

Masalah ini memengaruhi semua versi RES 2024.06 atau yang lebih lama

Mitigasi

Ikuti langkah-langkah ini untuk mengatasi masalah:

1. Untuk mengunduh skrip patch.py dan file group_member_sync_bug_fix.patch, jalankan perintah berikut, ganti <output-directory> dengan direktori lokal tempat Anda ingin mengunduh file, dan dengan versi RES yang ingin Anda tambal: <res_version>

Note

- [Skrip patch membutuhkan AWS CLI v2, Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
- Konfigurasi AWS CLI untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin S3 untuk menulis ke bucket yang dibuat oleh RES.
- Patch hanya mendukung versi RES 2024.04.02 dan 2024.06. Jika Anda menggunakan 2024.04 atau 2024.04.01, Anda dapat mengikuti langkah-langkah yang tercantum untuk memperbarui lingkungan Anda terlebih dahulu [Pembaruan versi minor](#) ke 2024.04.02 sebelum menerapkan tambalan.

- Versi RES: RES 2024.04.02

Tautan unduhan tambalan: [2024.04.02_group_member_sync_bug_fix.patch](#)

- Versi RES: RES 2024.06

Tautan unduhan tambalan: [2024.06_group_member_sync_bug_fix.patch](#)

```
OUTPUT_DIRECTORY=<output-directory>
```

```
RES_VERSION=<res_version>
```

```
mkdir -p ${OUTPUT_DIRECTORY}
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/  
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/  
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch  
--output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. Arahkan ke direktori tempat skrip patch dan file patch diunduh. Jalankan perintah patch berikut, ganti <environment-name> dengan nama lingkungan RES Anda:

```
cd ${OUTPUT_DIRECTORY}
```

```
ENVIRONMENT_NAME=<environment-name>
```

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. Untuk memulai ulang instance pengelola klaster untuk lingkungan Anda, jalankan perintah berikut:

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.06 dan sebelumnya) CVE-2024-6387, Regre, Kerentanan Keamanan di dan Ubuntu SSHion RHEL9 VDIs

Deskripsi bug

[CVE-2024-6387](#), dijuluki regreSSHion, telah diidentifikasi di server OpenSSH. Kerentanan ini memungkinkan penyerang jarak jauh dan tidak diautentikasi untuk mengeksekusi kode arbitrer pada server target, menghadirkan risiko parah pada sistem yang memanfaatkan OpenSSH untuk komunikasi yang aman.

Untuk RES, konfigurasi standar adalah melalui host bastion ke SSH ke desktop virtual, dan host bastion tidak terpengaruh oleh kerentanan ini. Namun, AMI default (Amazon Machine Image) yang kami sediakan RHEL9 dan Ubuntu2024 VDIs (Virtual Desktop Infrastructure) di ALL RES versi menggunakan versi OpenSSH yang rentan terhadap ancaman keamanan.

Ini berarti bahwa yang ada RHEL9 dan Ubuntu2024 VDIs dapat dieksploitasi, tetapi penyerang akan memerlukan akses ke host benteng.

Rincian lebih lanjut tentang masalah ini dapat ditemukan [di sini](#).

Versi yang terpengaruh

Masalah ini memengaruhi semua versi RES 2024.06 atau yang lebih lama.

Mitigasi

Keduanya RHEL9 dan Ubuntu telah merilis patch untuk OpenSSH yang memperbaiki kerentanan keamanan. Ini dapat ditarik menggunakan manajer paket masing-masing platform.

Jika Anda sudah ada RHEL9 atau Ubuntu VDIs, kami sarankan mengikuti VDIs petunjuk PATCH EXISTING di bawah ini. Untuk menambal future VDIs, sebaiknya ikuti VDIs petunjuk PATCH FUTURE. Instruksi ini menjelaskan cara menjalankan skrip untuk menerapkan pembaruan platform pada Anda VDIs.

PATCH YANG ADA VDIs

1. Jalankan perintah berikut yang akan menambal semua Ubuntu yang ada dan RHEL9 VDIs:
 - a. Skrip patch membutuhkan [AWS CLI v2](#).
 - b. Konfigurasi AWS CLI untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin AWS Systems Manager untuk mengirim perintah Systems Manager Run.

```
aws ssm send-command \  
  --document-name "AWS-RunRemoteScript" \  
  --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \  
  --parameters '{"sourceType":["S3"],"sourceInfo":[{"path":"https://  
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/  
patch_scripts/scripts/patch_openssh.sh"}],"commandLine":["bash  
patch_openssh.sh"]}'
```

2. Anda dapat memverifikasi skrip berjalan dengan sukses di [halaman Run Command](#). Klik pada tab Command History, pilih Command ID terbaru, dan verifikasi bahwa semua instance IDs memiliki pesan SUCCESS.

PATCH MASA DEPAN VDIs

1. Untuk mengunduh skrip patch dan file patch ([patch.py](#) dan [update_openssh.patch](#)) jalankan perintah berikut, ganti <output-directory> dengan direktori tempat Anda ingin mengunduh file, dan <environment-name> dengan nama lingkungan RES Anda:

Note

- Patch hanya berlaku untuk RES 2024.06.

- [Scrip patch membutuhkan AWS CLI v2\), Python 3.9.16 atau lebih tinggi, dan Boto3.](#)
- Konfigurasi salinan AWS CLI Anda untuk akun dan wilayah tempat RES digunakan, dan pastikan Anda memiliki izin S3 untuk menulis ke bucket yang dibuat oleh RES.

```
OUTPUT_DIRECTORY=<output-directory>
```

```
ENVIRONMENT_NAME=<environment-name>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. Jalankan perintah patch berikut:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. Mulai ulang instance VDC Controller untuk lingkungan Anda dengan perintah berikut:

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

Important

Patching future hanya VDIs didukung pada RES versi 2024.06 dan yang lebih baru. Untuk menambal future VDIs di lingkungan RES dengan versi lebih awal dari 2024.06, pertama-

tama tingkatkan lingkungan RES ke 2024.06 menggunakan instruksi di: [Pembaruan versi utama](#)

.....

Pemberitahuan

Setiap EC2 instans Amazon dilengkapi dengan dua lisensi Layanan Desktop Jarak Jauh (Layanan Terminal) untuk tujuan administrasi. [Informasi](#) ini tersedia untuk membantu Anda memberikan lisensi ini untuk administrator Anda. Anda juga dapat menggunakan [AWS Systems Manager Session Manager](#), yang memungkinkan login jarak jauh ke EC2 instans Amazon tanpa RDP dan tanpa memerlukan lisensi RDP. Jika lisensi Layanan Desktop Jarak Jauh tambahan diperlukan, pengguna Remote Desktop CALs harus dibeli dari Microsoft atau pengecer lisensi Microsoft. Pengguna Remote Desktop CALs dengan Jaminan Perangkat Lunak aktif memiliki manfaat Mobilitas Lisensi dan dapat dibawa ke AWS lingkungan penyewa default (bersama). Untuk informasi tentang membawa lisensi tanpa Jaminan Perangkat Lunak atau manfaat Mobilitas Lisensi, silakan lihat [bagian FAQ ini](#).

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat. AWS tanggung jawab dan kewajiban kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Research and Engineering Studio on AWS dilisensikan berdasarkan ketentuan Lisensi Apache Versi 2.0 yang tersedia di [The Apache Software](#) Foundation.

Revisi

Untuk informasi selengkapnya, lihat file [changeLog.md](#) di repositori. GitHub

Tanggal	Perubahan
Desember 2024	- Versi rilis 2024.12 Ditambahkan bagian - Sinkronisasi Direktori Aktif. Mengkonfigurasi Izin Desktop. Mengkonfigurasi akses browser File. Mengkonfigurasi akses SSH. Menyiapkan pengguna Amazon Cognito. Bagian berubah - Batas lingkungan. Konfigurasi VPC pribadi (opsional).
Oktober 2024	- Versi rilis 2024.10: Ditambahkan dukungan untuk - Batas lingkungan. Profil berbagi desktop. Antarmuka desktop virtual autostop.
Agustus 2024	- Versi rilis 2024.08: Ditambahkan dukungan untuk - - memasang bucket Amazon S3 ke instance Linux Virtual Desktop Infrastructure (VDI). Lihat Bucket Amazon S3. - izin proyek khusus, model izin yang disempurnakan yang memungkinkan penyesuaian peran yang ada dan penambahan peran khusus. Lihat Kebijakan izin.

Tanggal	Perubahan
	Panduan Pengguna: memperluas Pemecahan Masalah bagian.
Juni 2024	- Versi rilis 2024.06 - Dukungan Ubuntu, izin pemilik Proyek. - Panduan Pengguna: ditambahkan Buat lingkungan demo
April 2024	Versi rilis 2024.04 - Templat peluncuran proyek siap RES AMIs dan
Maret 2024	Topik pemecahan masalah tambahan, retensi CloudWatch Log, hapus instalasi versi minor
Februari 2024	Versi rilis 2024.01.01 - template penyebaran diperbarui
Januari 2024	Versi rilis 2024.01
Desember 2023	GovCloud arah dan template ditambahkan
November 2023	Rilis awal

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