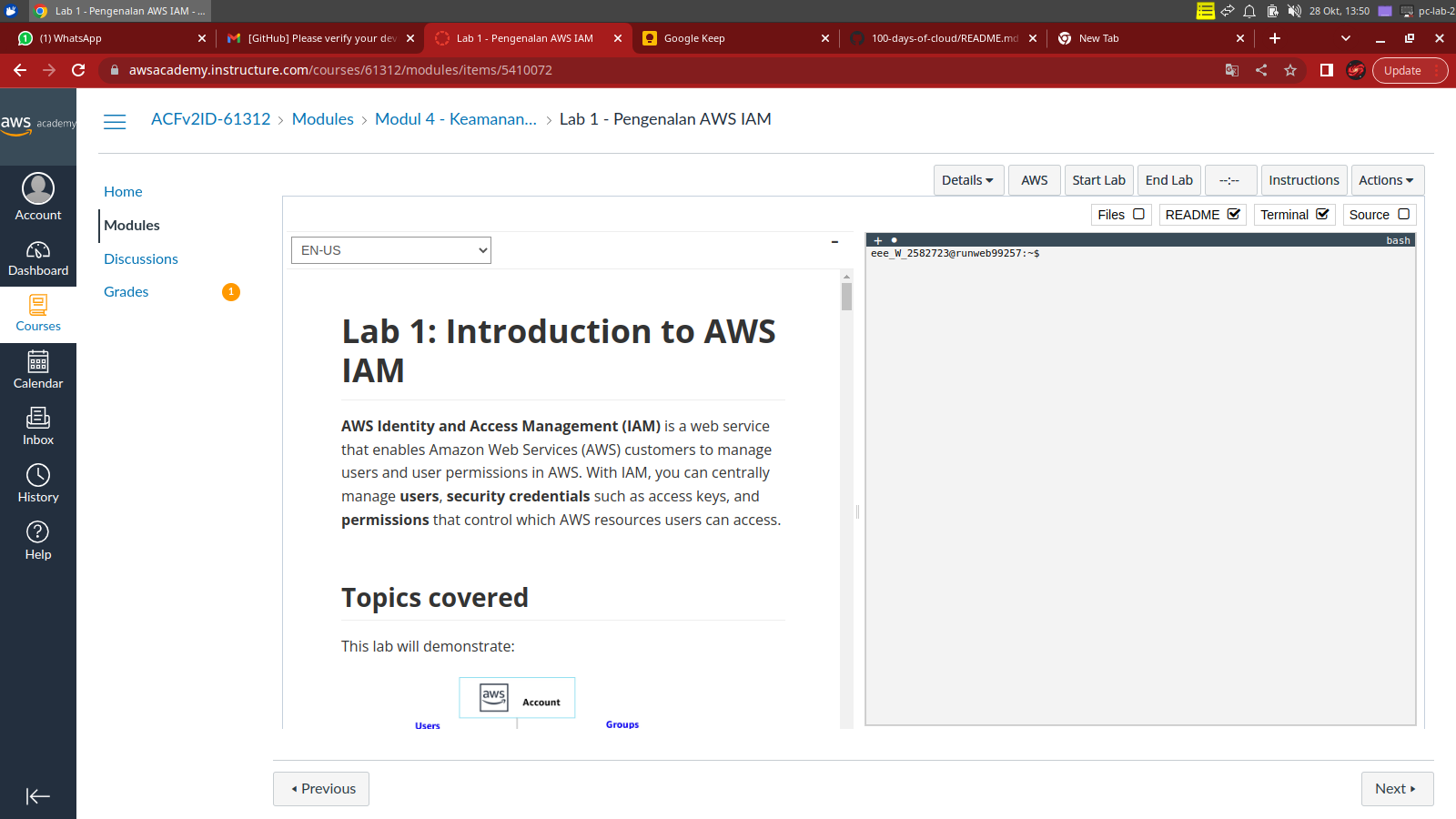
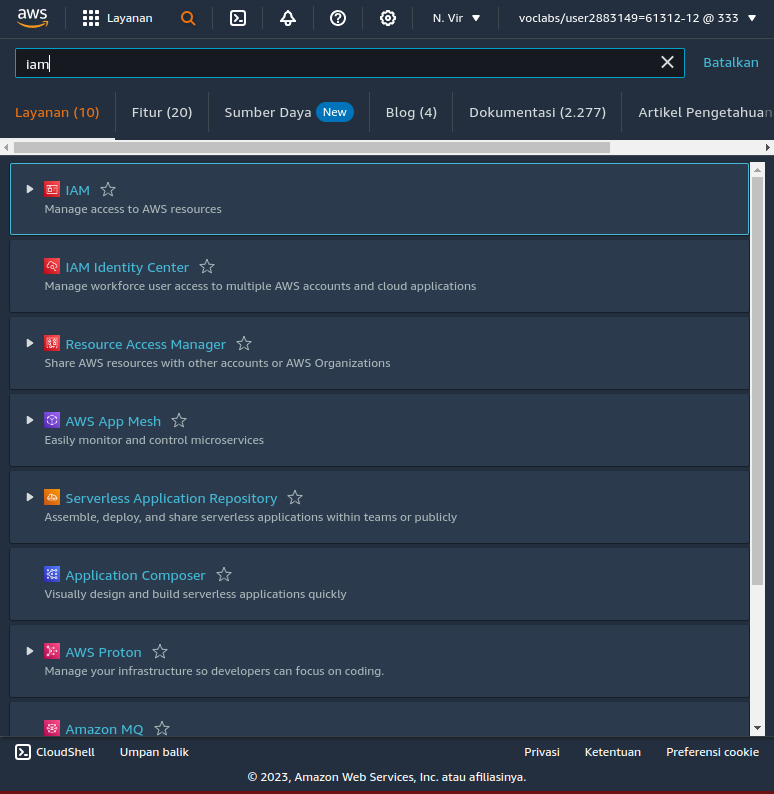
**LAB 1 : IAM**

1. Di Bagian atas, pilih Mulai Lab untuk memulai lab.
2. Tunggu sampai Anda melihat pesan "Status lab: siap", lalu klik X untuk menutup panel Mulai Lab.
3. Di bagian atas instruksi ini, pilih AWS. Tindakan ini akan membuka Konsol Manajemen AWS di tab browser baru. Anda akan login ke sistem secara otomatis

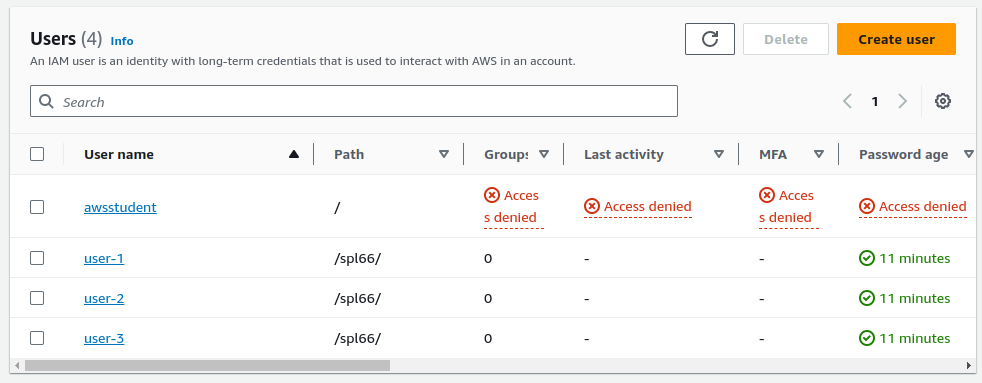


1. Di AWS Management Console, di menu Layanan, pilih IAM.

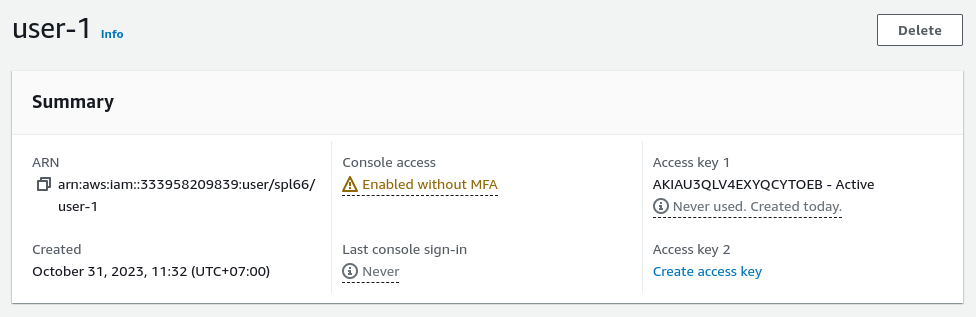


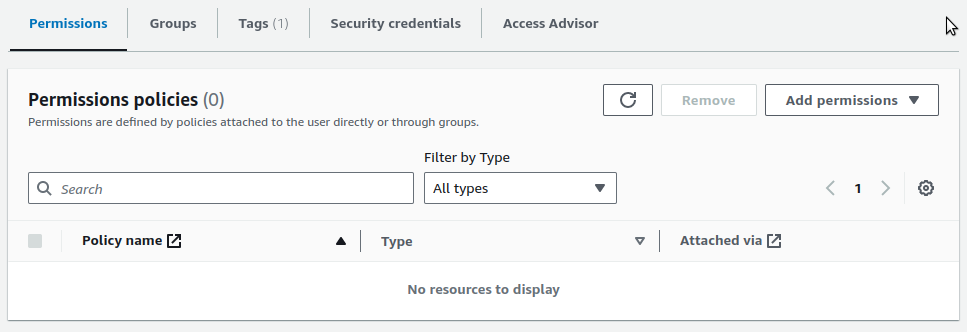
1. Di panel navigasi kiri, pilih Pengguna.Pengguna IAM berikut telah dibuat :

* user-1
* user-2
* user-3

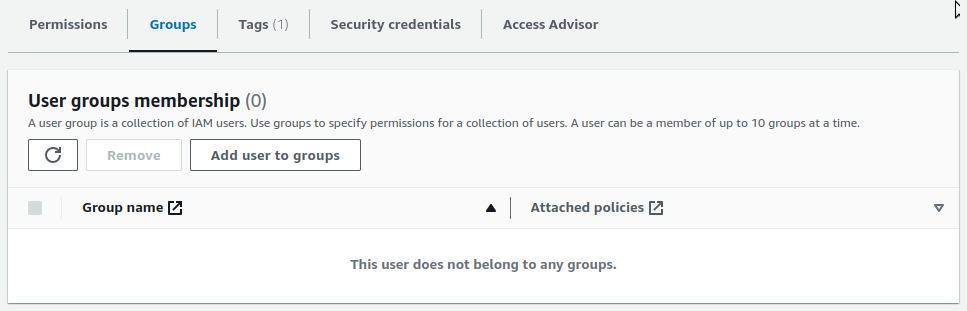


1. Pilih user-1. Ini akan membawa Anda ke halaman ringkasan untuk user-1. Tab Izin akan ditampilkan. Pastikan user-1 tidak memiliki izin apa pun.

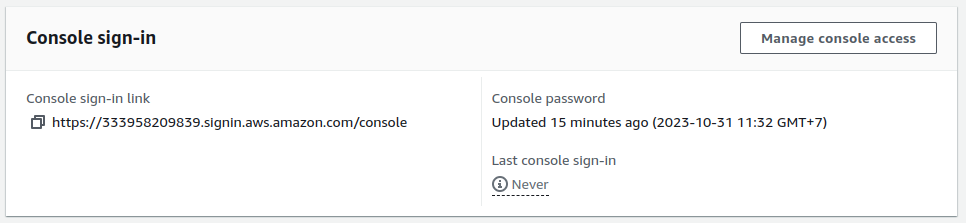




1. Pilih tab Grup. user-1 juga bukan anggota dari grup mana pun.

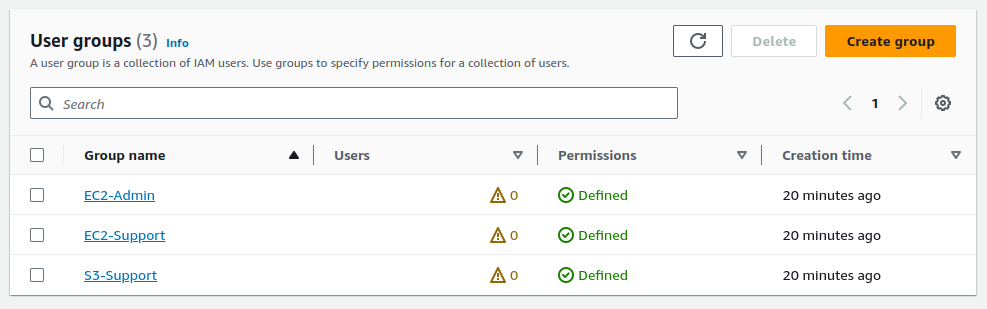


1. Pilih tab Kredensial keamanan. user-1 diberikan Kata sandi konsol

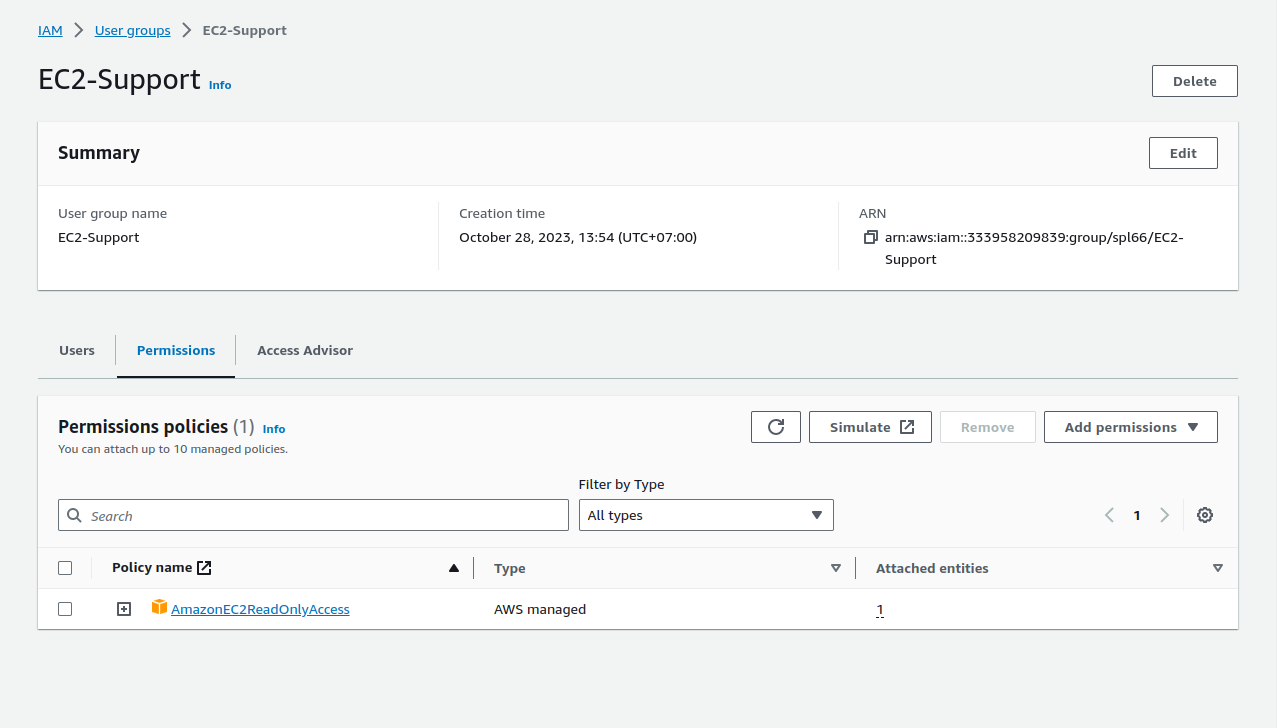


1. Di panel navigasi kiri, pilih Grup pengguna. Grup berikut telah dibuat untuk Anda:

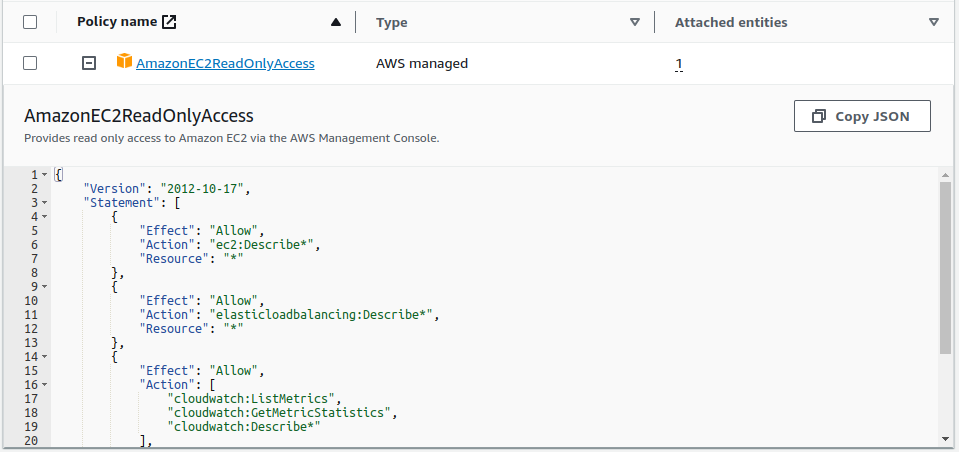
* EC2-Admin
* EC2-Support
* S3-Support



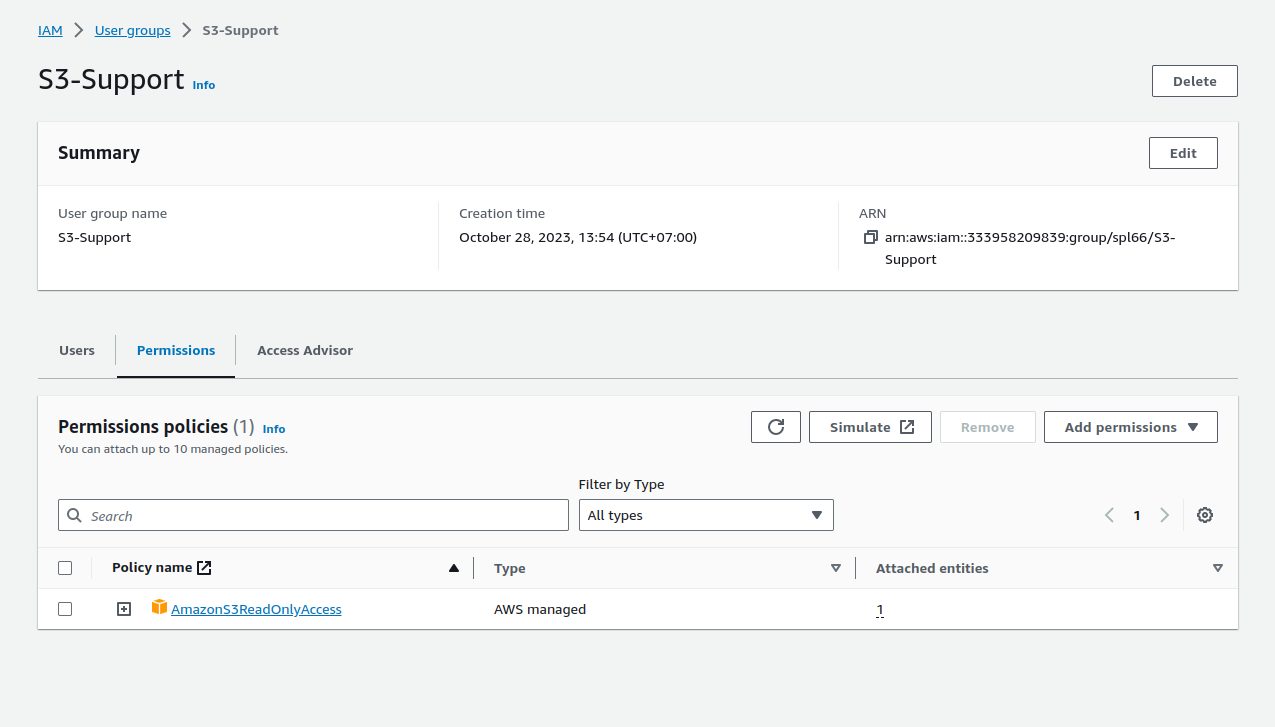
1. Pilih grup EC2-Support. Ini akan membawa Anda ke halaman ringkasan untuk grup EC2-Support.
2. Pilih tab Izin. Grup ini memiliki Kebijakan Terkelola terkait, yang disebut AmazonEC2ReadOnlyAccess. Kebijakan yang Dikelola adalah kebijakan yang dibangun sebelumnya (yang dibangun oleh AWS atau oleh administrator Anda) yang dapat dipasangkan ke Pengguna dan Grup IAM. Saat kebijakan tersebut diperbarui, perubahan kebijakan akan segera berlaku terhadap semua Pengguna dan Grup yang dipasangkan pada kebijakan (i ain’t reading allat).



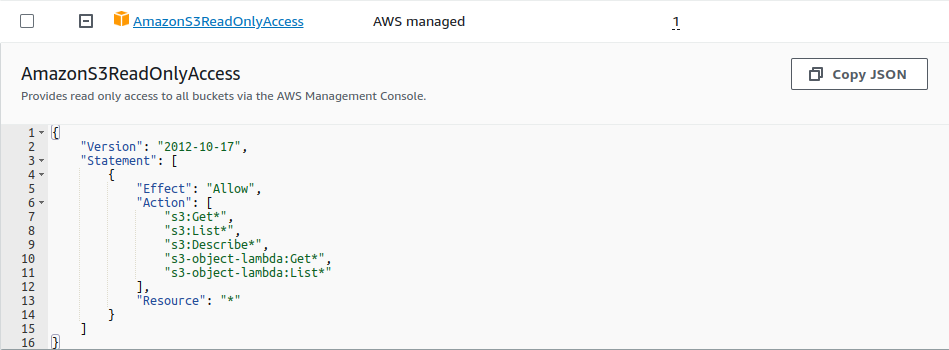
1. Pilih ikon plus (+) di sebelah kebijakan AmazonEC2ReadOnlyAccess untuk melihat detail kebijakan.



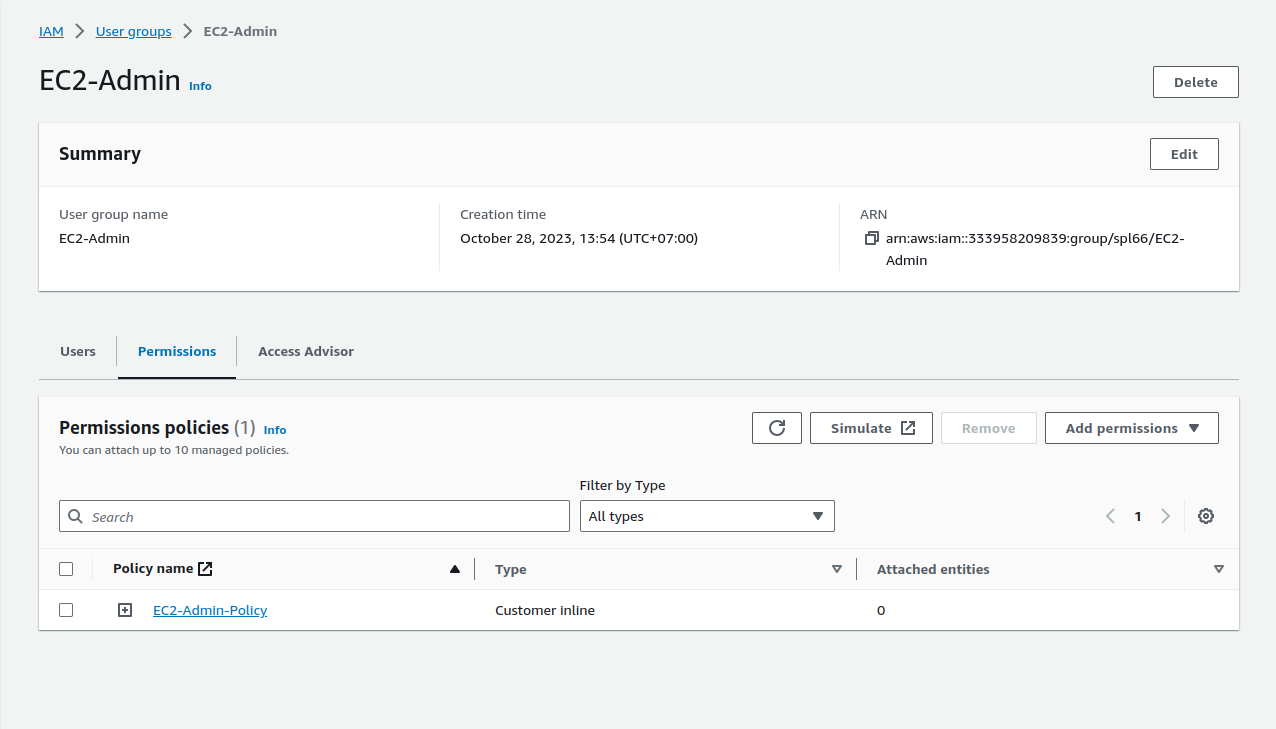
1. Pilih ikon minus (-) untuk menyembunyikan detail kebijakan.
2. Di panel navigasi kiri, pilih Grup pengguna. Pilih grup S3-Support lalu pilih tab Izin. Grup S3-Support memiliki lampiran kebijakan AmazonS3ReadOnlyAccess.



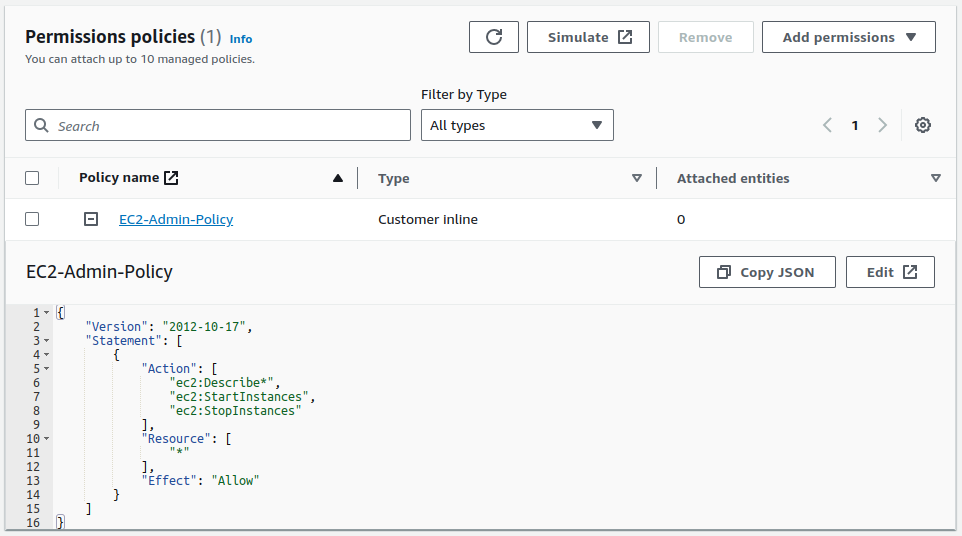
1. Pilih ikon plus (+) untuk melihat detail kebijakan. Kebijakan ini memberikan izin untuk Mendapatkan dan Mencantumkan sumber daya di Amazon S3.



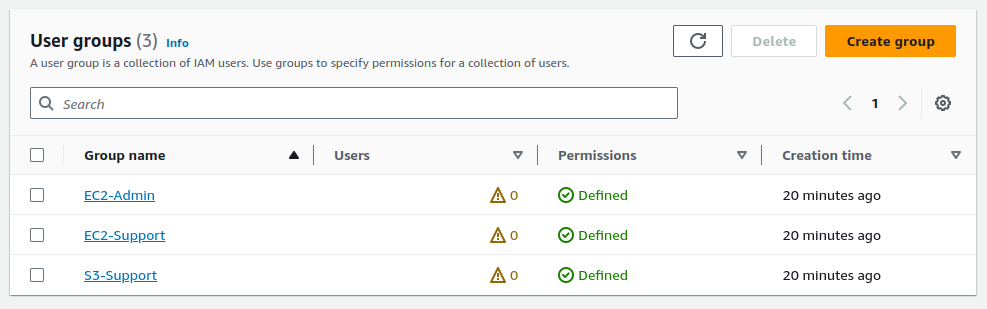
1. Pilih ikon minus (-) untuk menyembunyikan detail kebijakan.
2. Di panel navigasi kiri, pilih Grup pengguna. Pilih grup EC2-Admin lalu pilih tab Izin. Grup ini sedikit berbeda dari dua grup lainnya. Alih-alih Kebijakan yang Dikelola, grup ini memiliki Kebijakan Inline, yakni kebijakan yang ditetapkan ke satu Pengguna atau Grup saja. Kebijakan Inline biasanya digunakan untuk menerapkan izin untuk situasi yang hanya akan terjadi sekali.



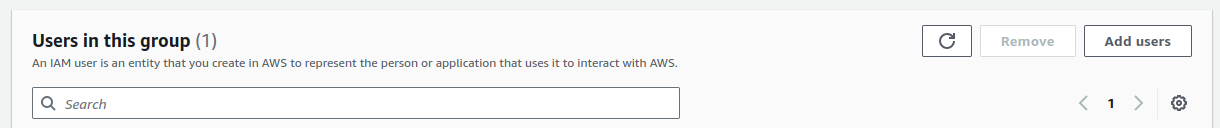
1. Pilih ikon plus (+) untuk melihat detail kebijakan. Kebijakan ini memberikan izin untuk melihat (Mendeskripsikan) informasi tentang Amazon EC2 serta kemampuan untuk Memulai dan Menghentikan instans.



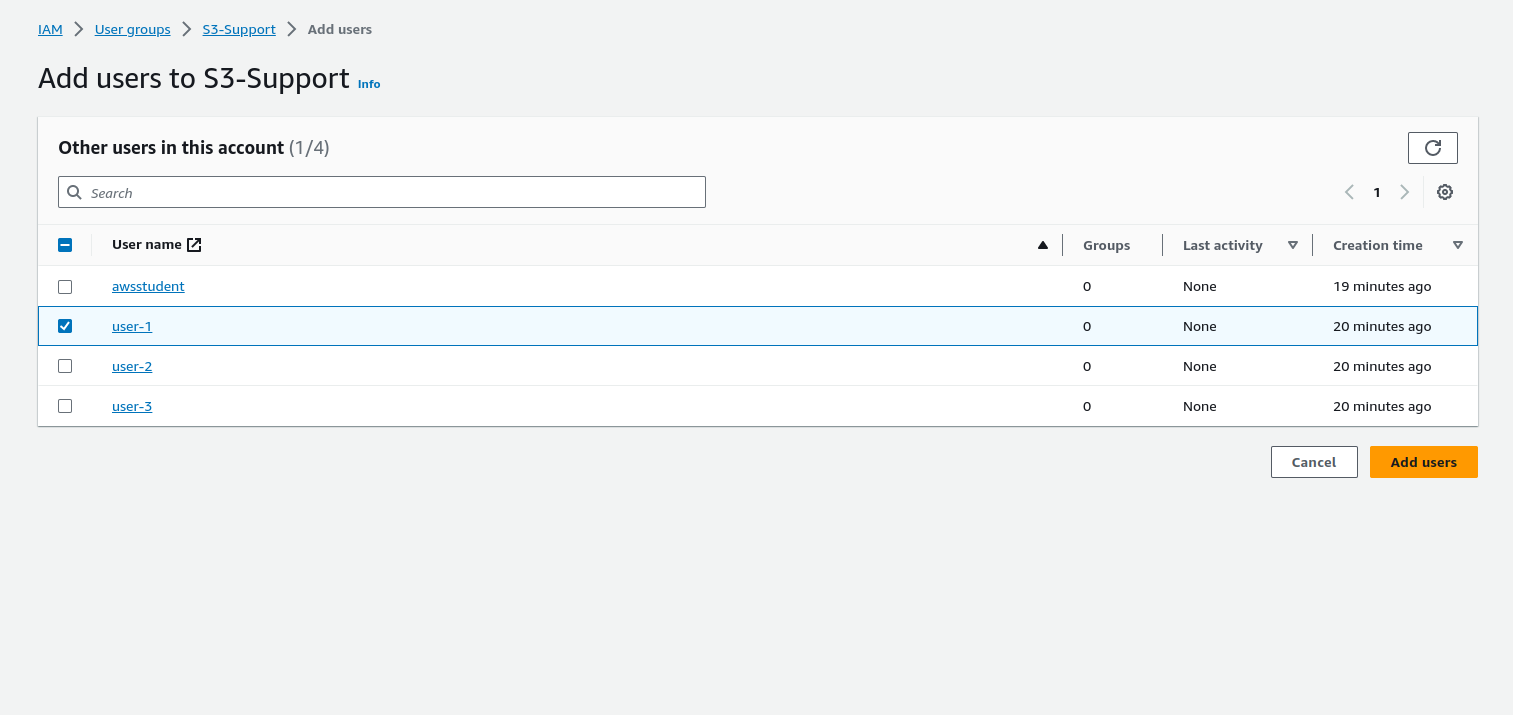
1. Pilih ikon minus (-) untuk menyembunyikan detail kebijakan.
2. Menambahkan user-1 ke Grup S3-Support, Di panel navigasi kiri, pilih Grup pengguna.

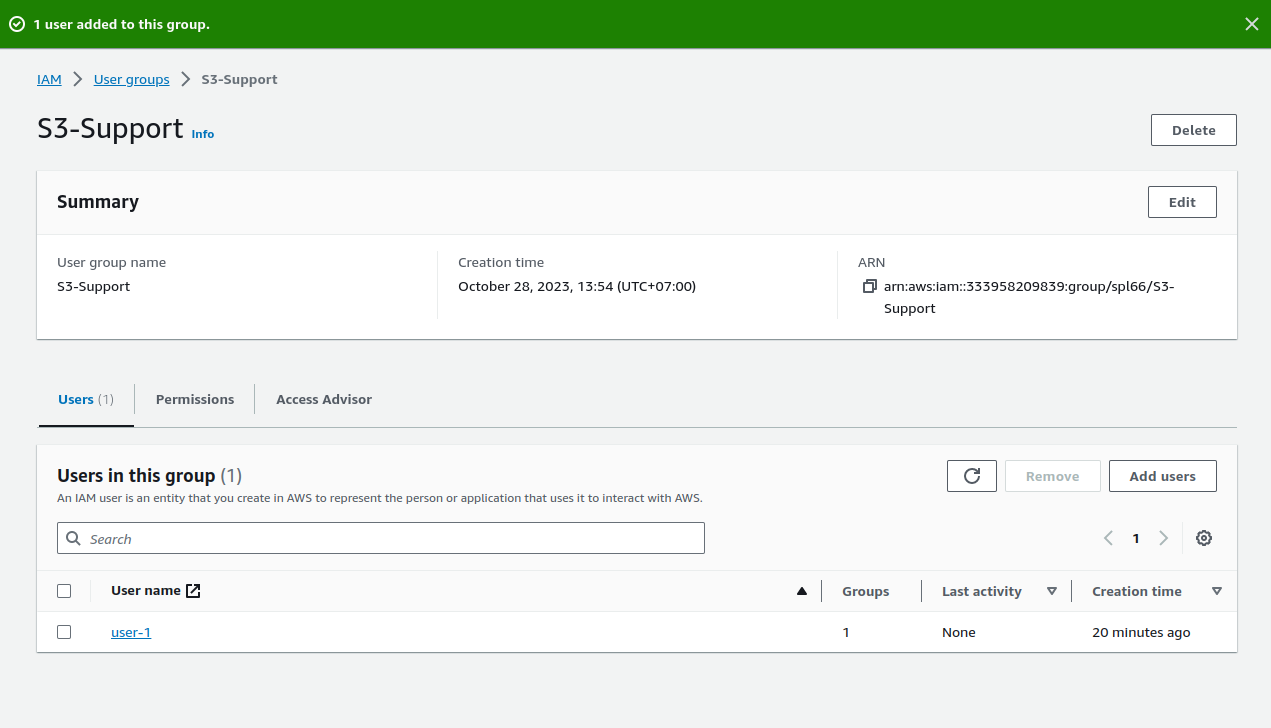


1. PIlih grup S3-Support.
2. Pada tab Pengguna, pilih Tambahkan pengguna.

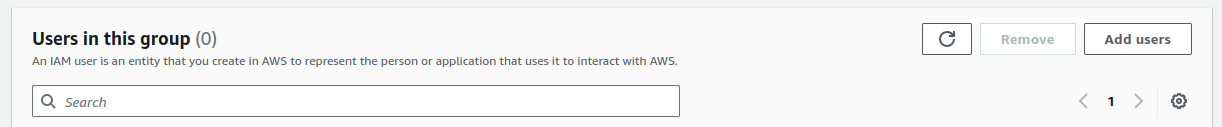


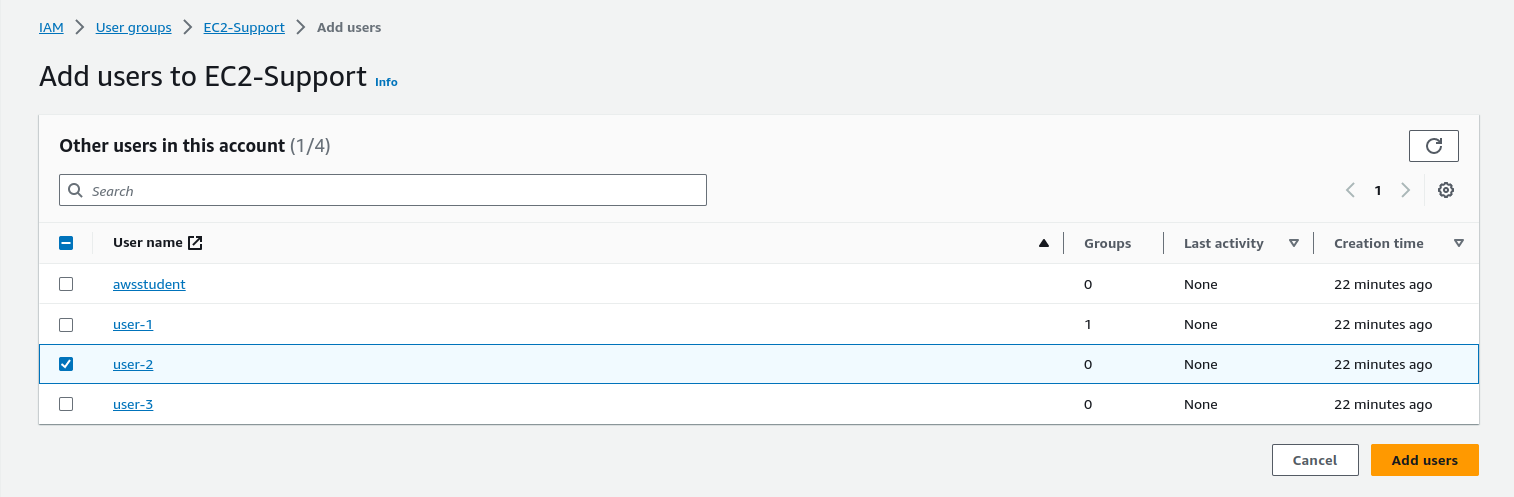
1. Di jendela Tambahkan pengguna ke S3-Support, pilih user-1. Di bagian bawah layar, pilih Tambahkan Pengguna.

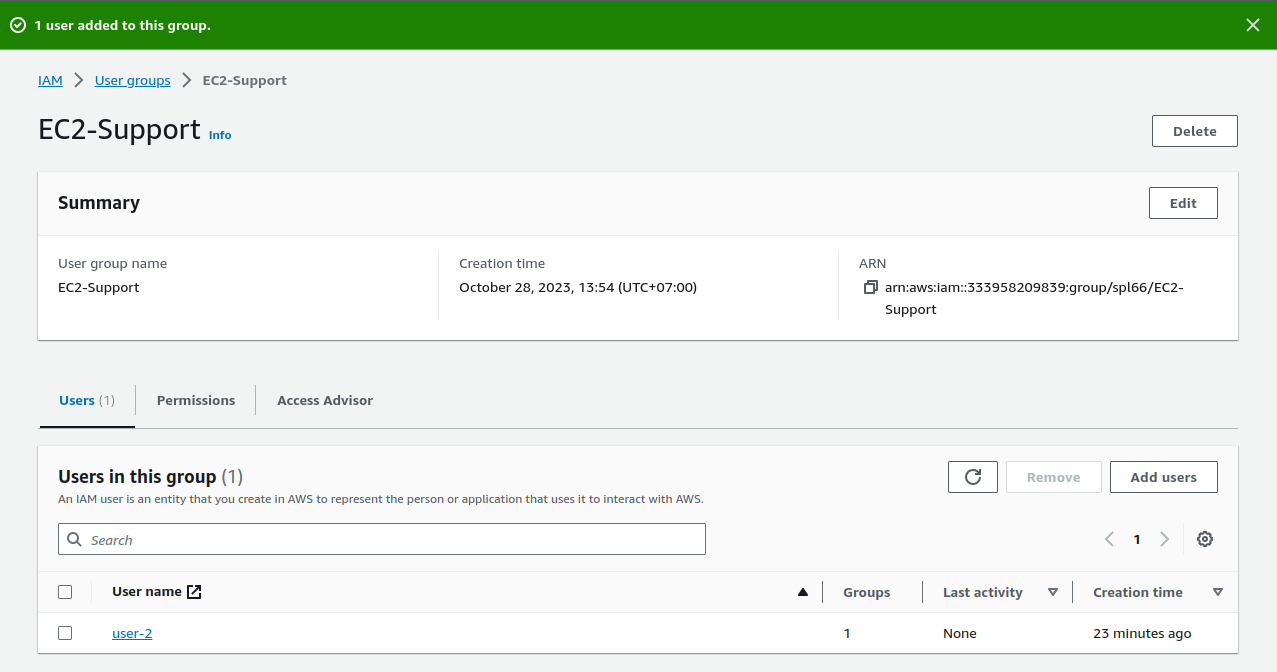




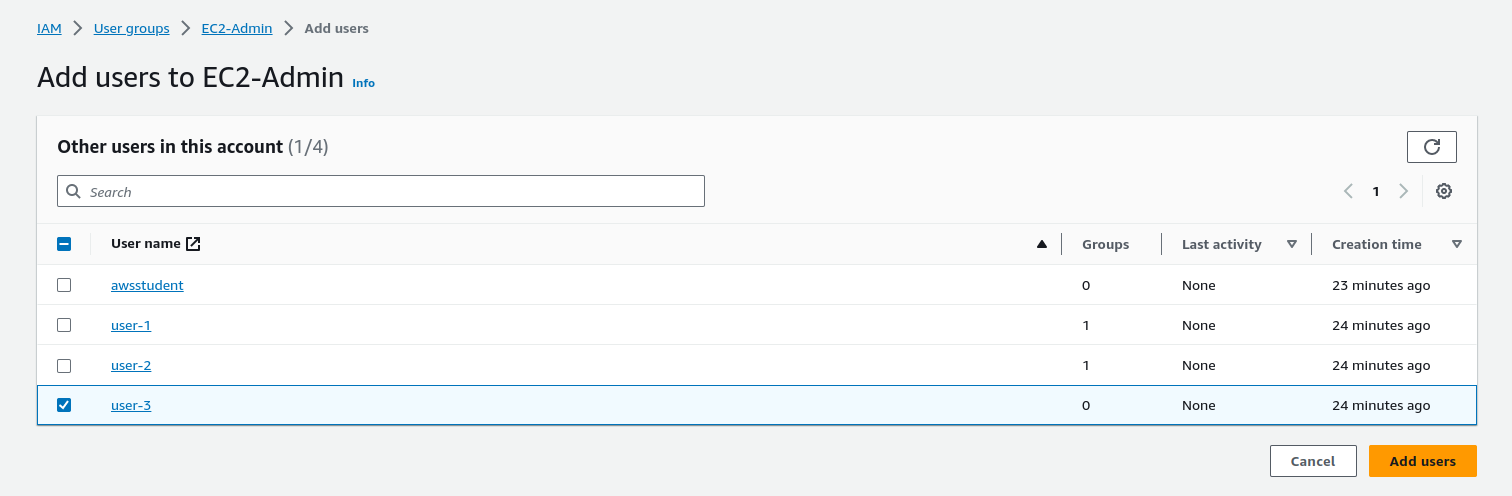
1. Menggunakan langkah-langkah yang sama dengan yang di atas, tambahkan user-2 ke grup EC2-Support. user-2 seharusnya telah menjadi bagian dari grup EC2-Support.

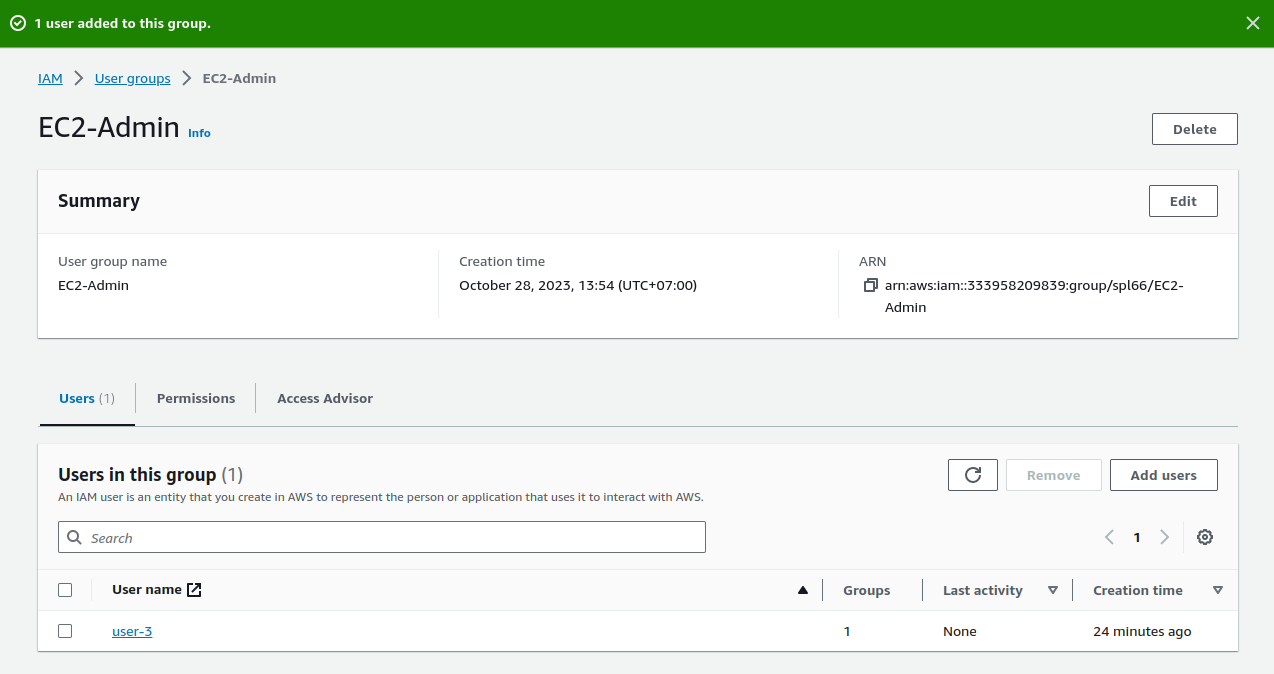




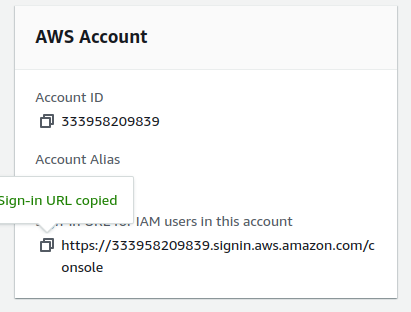


1. Menggunakan langkah-langkah yang sama dengan yang di atas, tambahkan user-3 ke grup EC2-Admin. user-3 seharusnya telah menjadi bagian dari grup EC2-Admin.



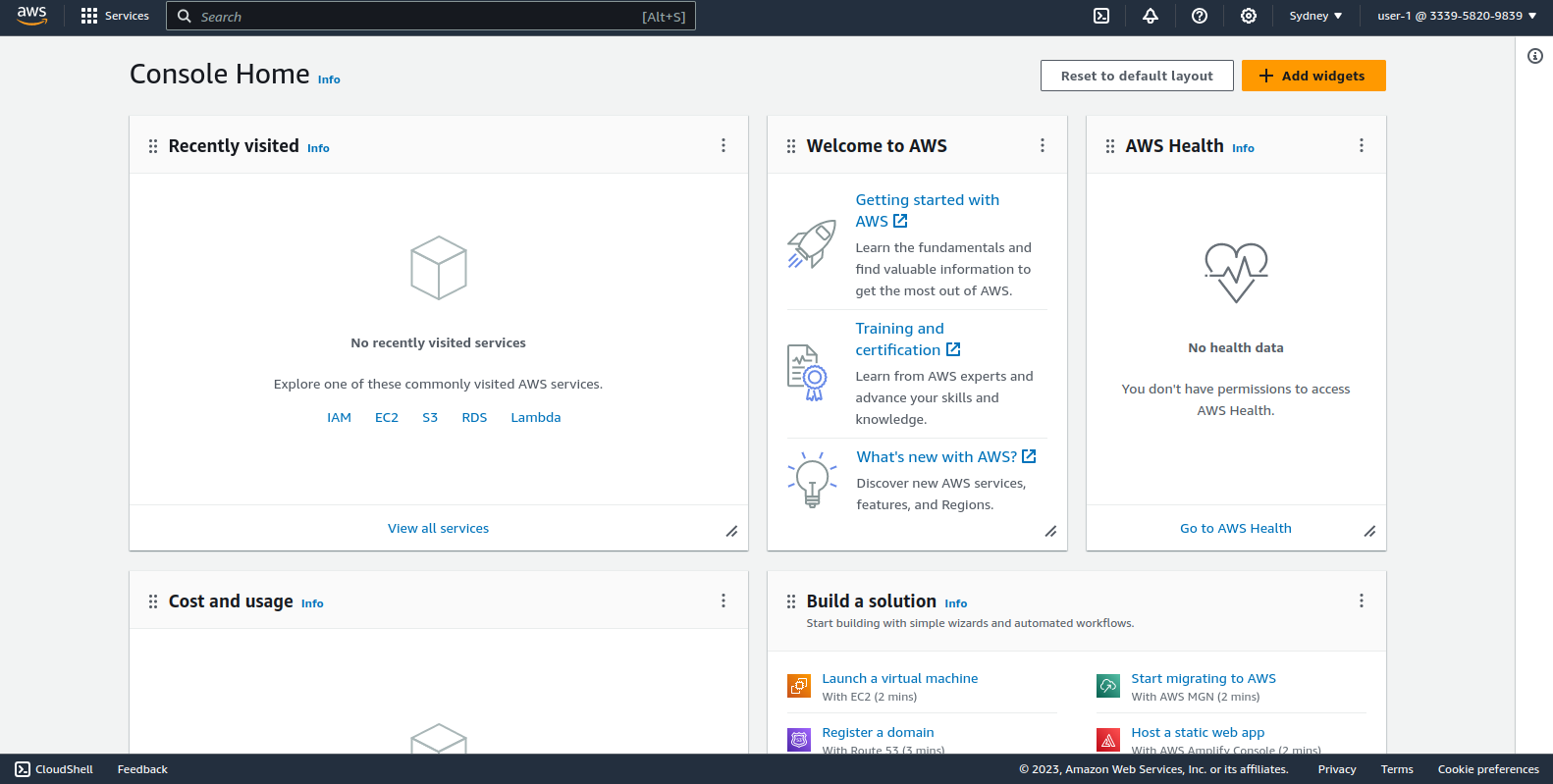


1. Di panel navigasi kiri, pilih Dasbor. Salin URL masuk untuk pengguna IAM dalam akun ini ke editor teks.

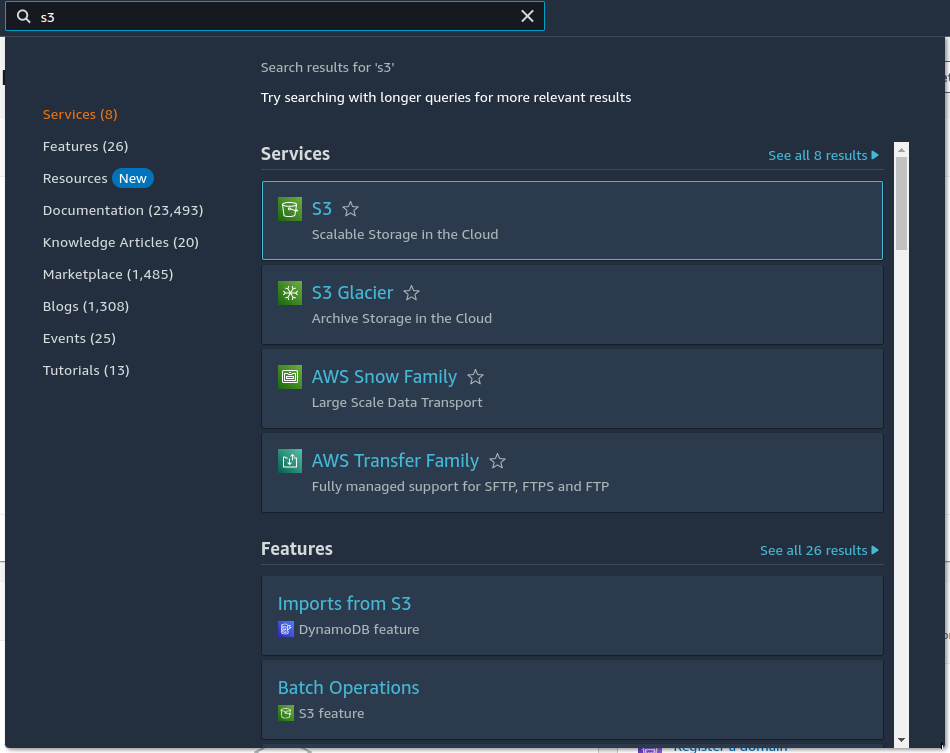


1. Masuk dengan:

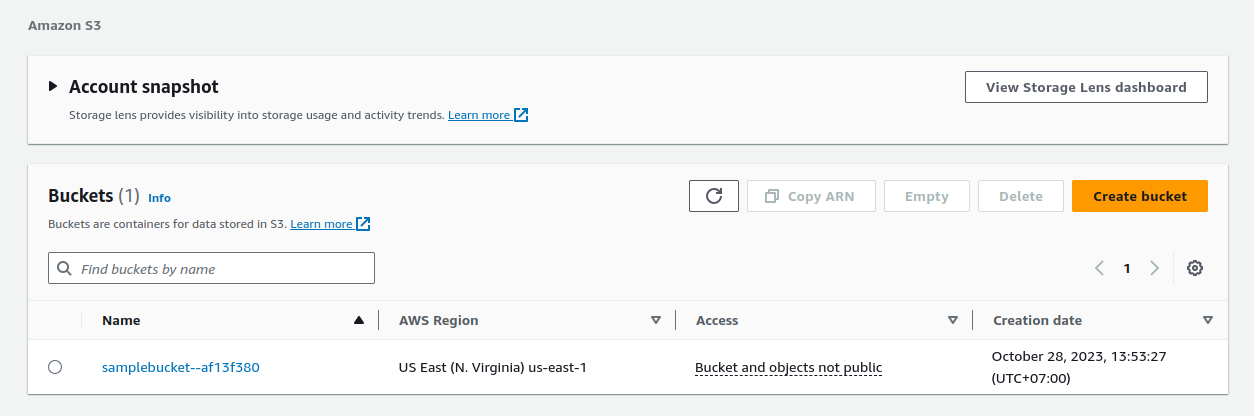
* Nama pengguna IAM: user-1
* Kata sandi: Lab-Password1

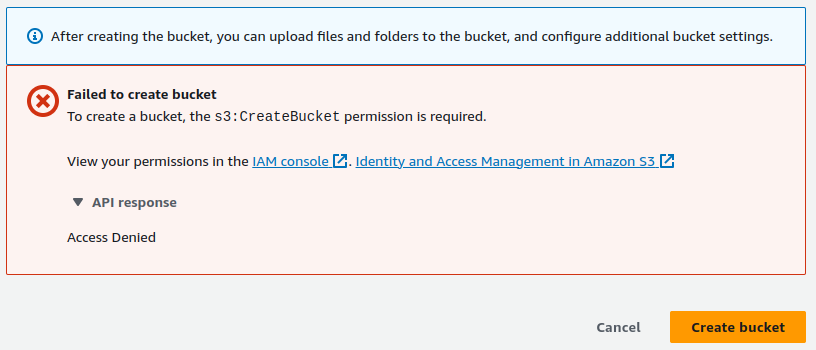


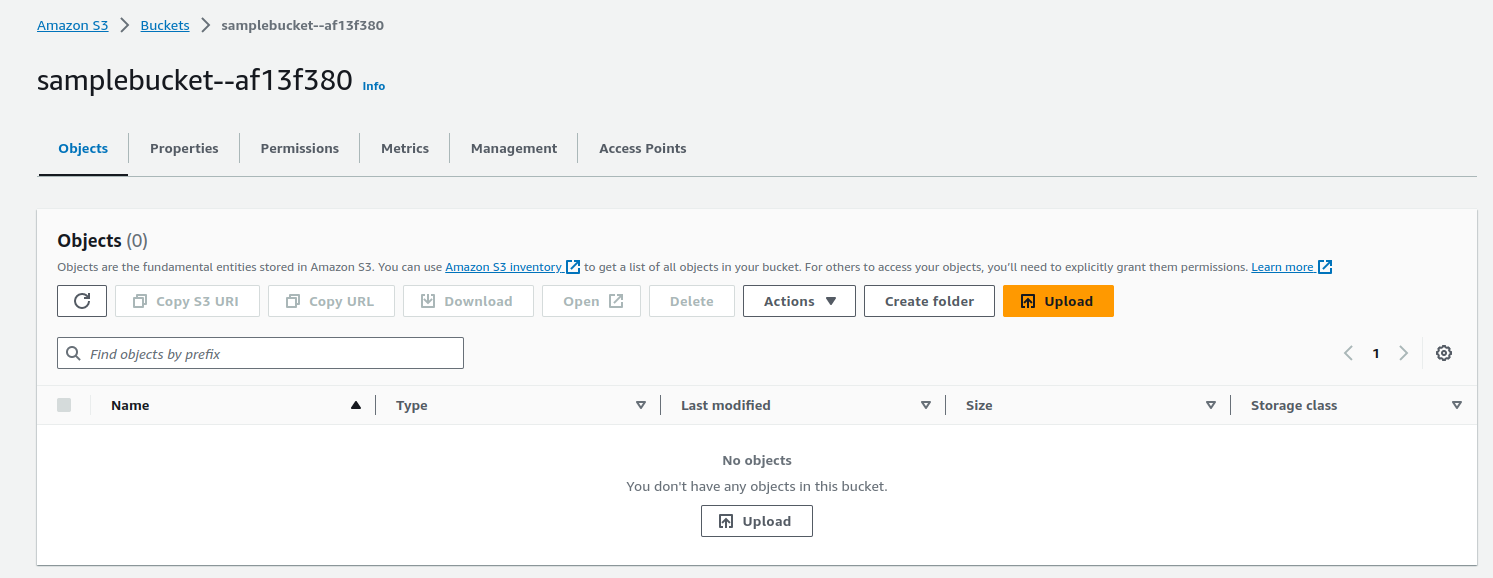
1. Di menu Layanan, pilih S3.

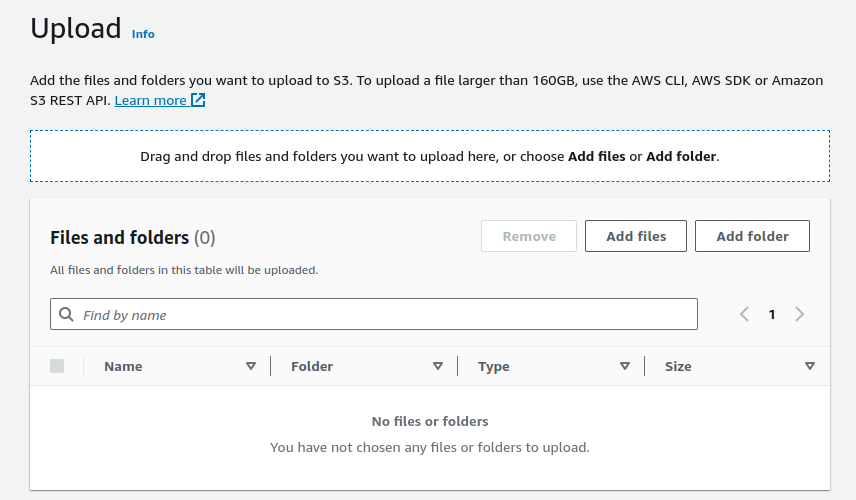


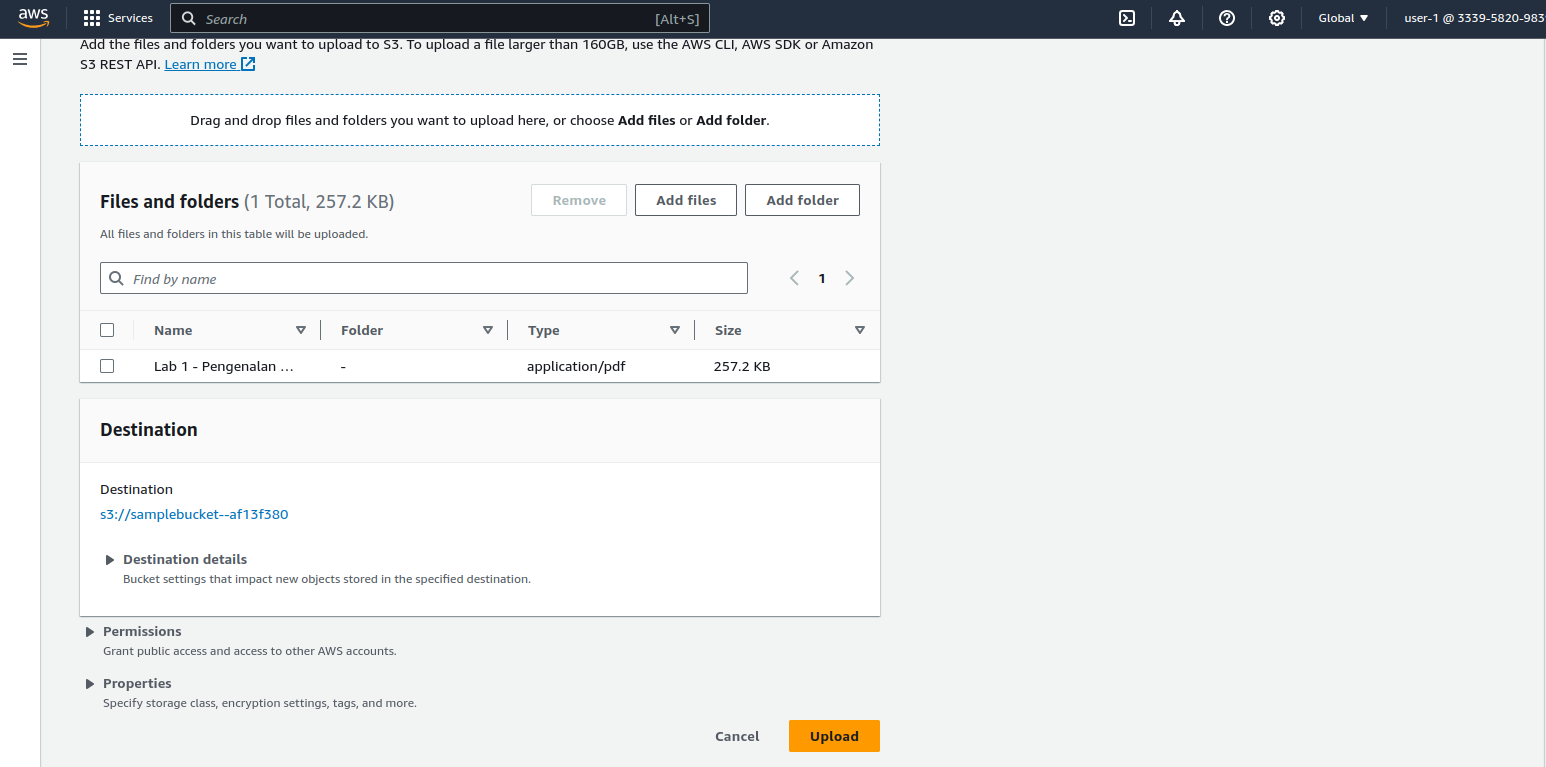
1. Pilih nama bucket yang ada di dalam akun dan telusuri kontennya. Karena pengguna Anda adalah bagian dari Grup S3-Support di IAM, mereka memiliki izin untuk melihat daftar bucket Amazon S3 dan kontennya. Sekarang, uji apakah mereka memiliki akses ke Amazon EC2.

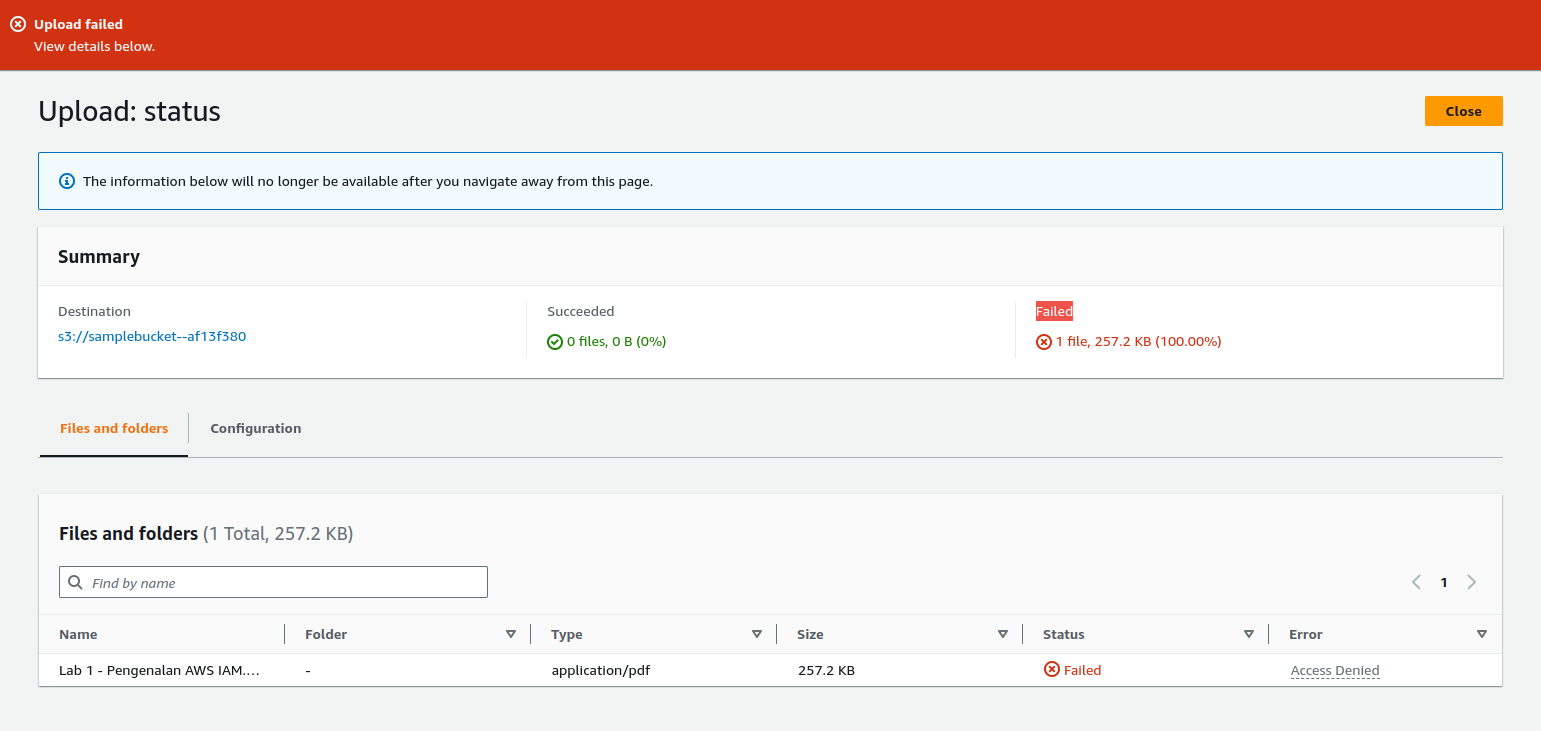




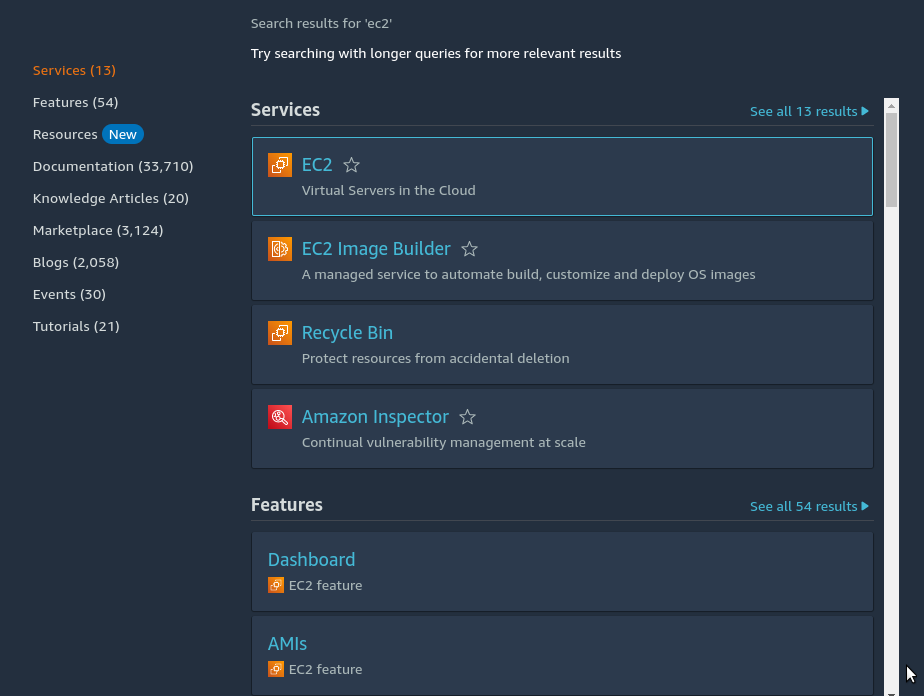




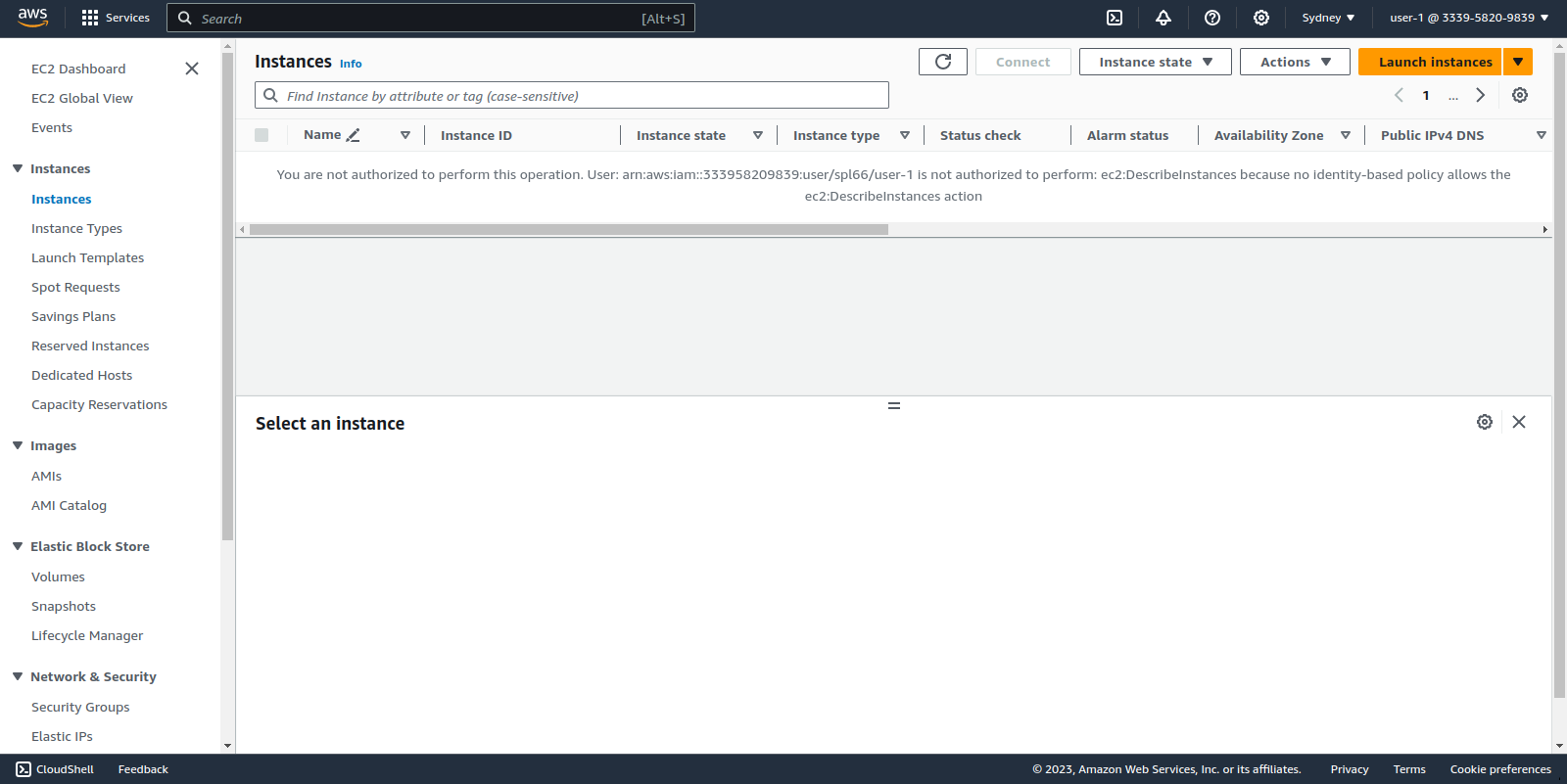




1. Pada menu Layanan, pilih EC2.



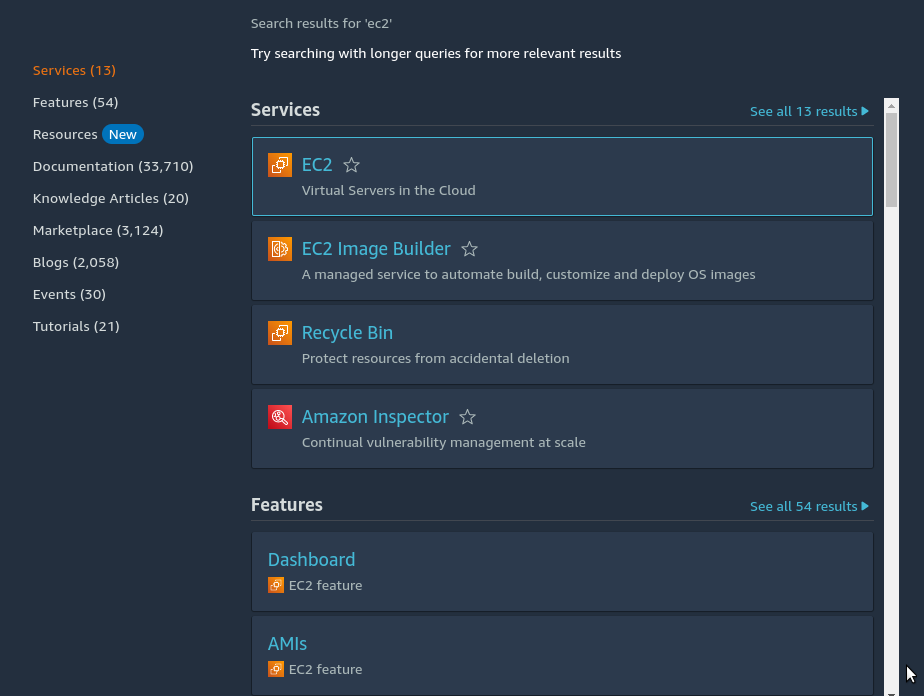
1. Di panel navigasi kiri, pilih Instans. Anda tidak dapat melihat instans apa pun. Sebagai gantinya, Anda melihat pesan Anda tidak diotorisasi untuk melakukan operasi ini. Hal ini dikarenakan pengguna ini belum diberi izin untuk mengakses Amazon EC2. Anda akan masuk sebagai user-2, yang telah direkrut sebagai staf dukungan Amazon EC2 Anda.



1. Keluarkan user-1 dari AWS Management Console dengan menyelesaikan tindakan berikut:

* Di bagian atas layar, pilih user-1
* Pilih Keluar

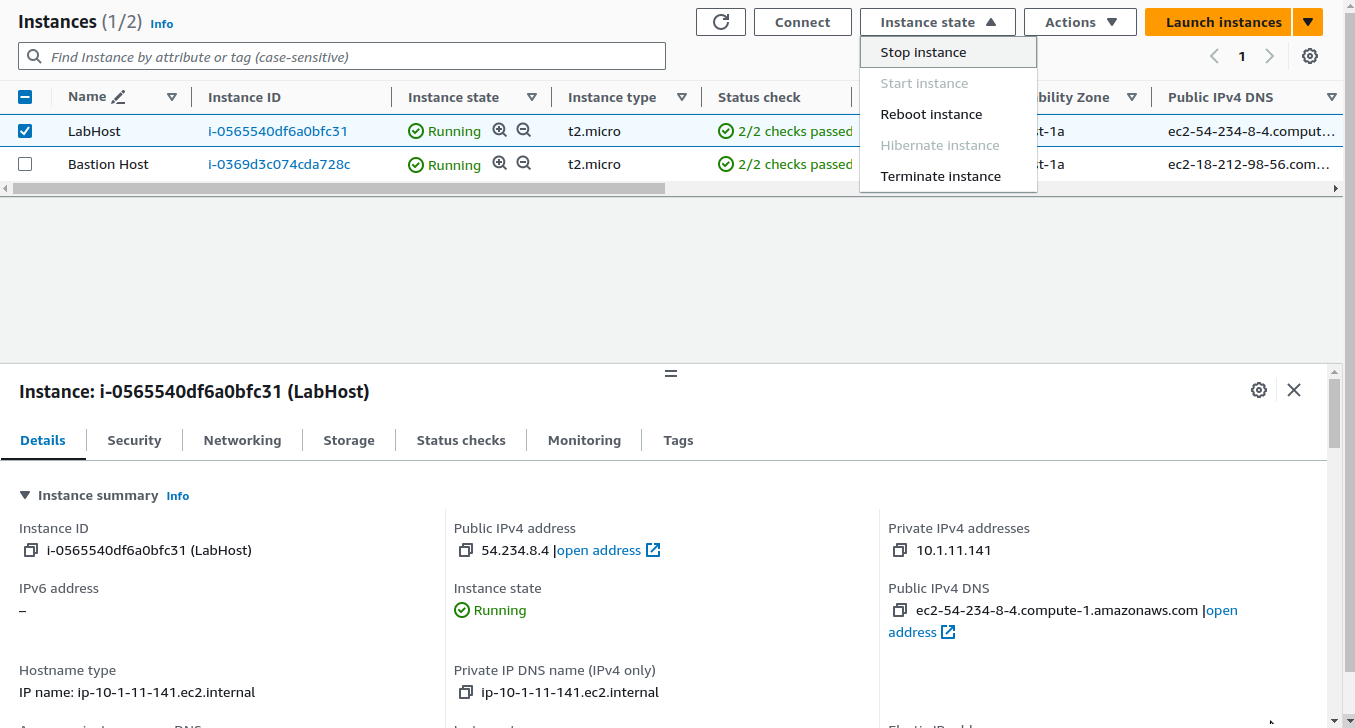
1. Tempelkan tautan Masuk pengguna IAM ke dalam bilah alamat tab browser pribadi Anda dan tekan Enter.
2. Pada menu Layanan, pilih EC2.



1. Di panel navigasi kiri, pilih Instans. Anda sekarang dapat melihat instans Amazon EC2 karena Anda memiliki izin Hanya Baca. Namun, Anda tidak akan dapat membuat perubahan ke sumber daya Amazon EC2.
2. Jika Anda tidak dapat melihat instans Amazon EC2, Wilayah Anda mungkin salah. Di kanan atas layar, tarik ke bawah menu Region dan pilih region yang Anda perhatikan di bagian atas lab (misalnya, N. Virginia).



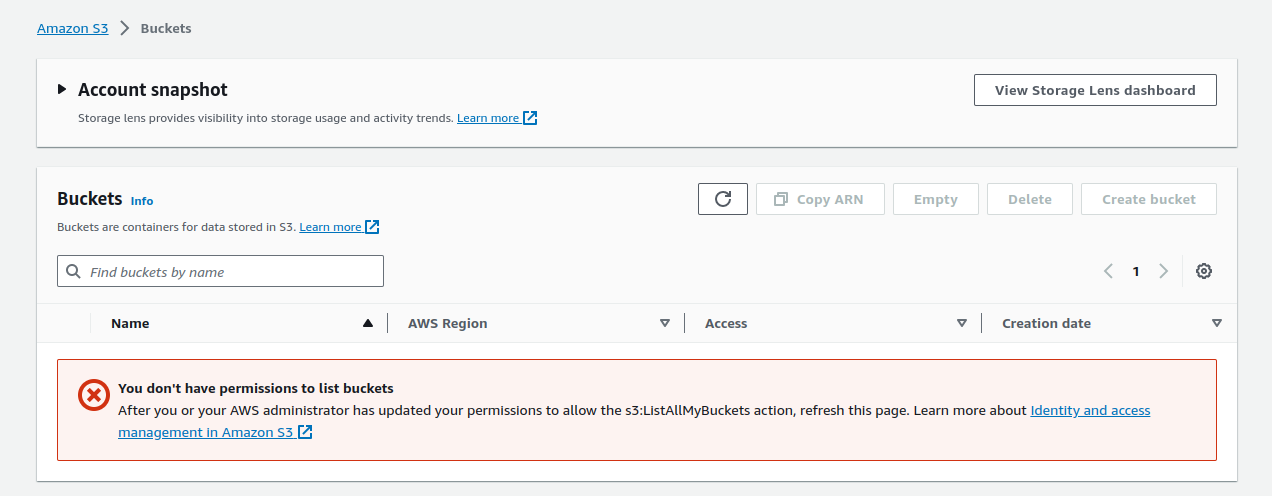
1. Pilih instans dengan nama LabHost.



1. Di menu Status instans di atas, pilih Hentikan instans. Di jendela Hentikan Instans, pilih Hentikan. Anda akan menerima pesan kesalahan Anda tidak diotorisasi untuk melakukan operasi ini. Ini menunjukkan bahwa kebijakan hanya mengizinkan Anda melihat informasi, tanpa membuat perubahan.



1. Pilih X untuk menutup pesan Gagal menghentikan instans. Selanjutnya, periksa apakah user-2 dapat mengakses Amazon S3.
2. Di Layanan, pilih S3. Anda akan melihat pesan Anda tidak memiliki izin untuk mencantumkan bucket karena user-2 tidak memiliki izin untuk mengakses Amazon S3.



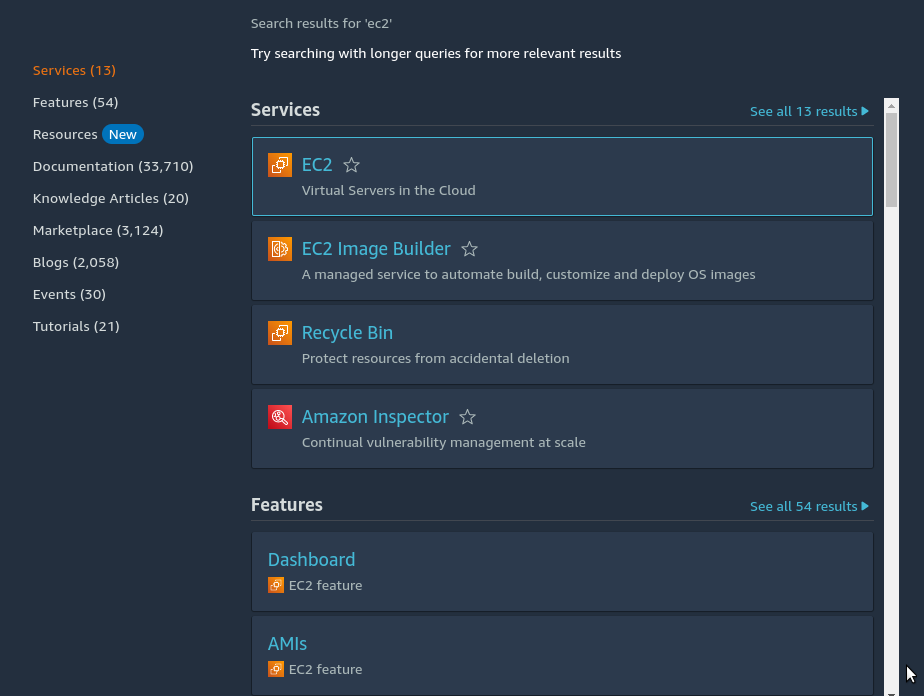
1. Keluarkan user-2 dari AWS Management Console dengan menyelesaikan tindakan berikut:

* Di bagian atas layar, pilih user-2
* Pilih Keluar

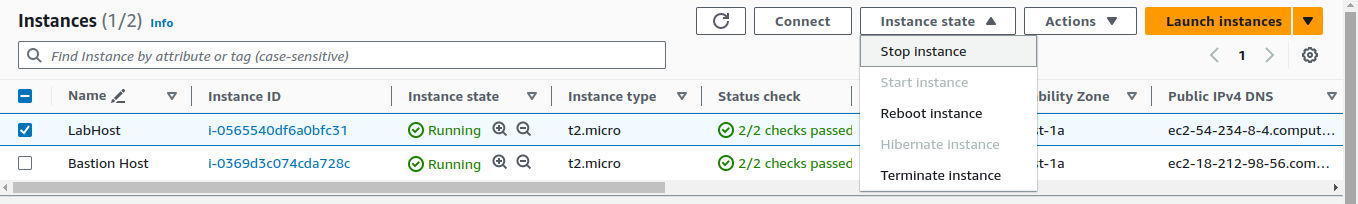
1. Tempelkan tautan Masuk pengguna IAM ke jendela pribadi Anda dan tekan Enter. Lalu tempelkan tautan masuk ke dalam bilah alamat tab browser web pribadi Anda lagi.
2. Masuk dengan:

* Nama pengguna IAM: user-3
* Kata sandi: Lab-Password3

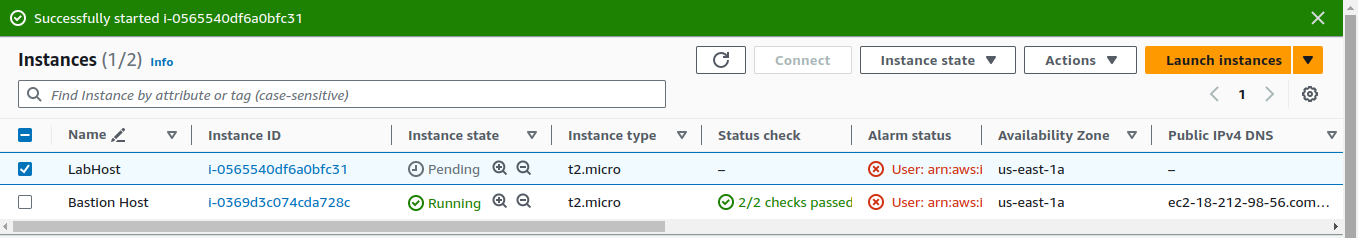
1. Pada menu Layanan, pilih EC2.



1. Di panel navigasi kiri, pilih Instans. Sebagai Administrator EC2, Anda sekarang seharusnya memiliki izin untuk menghentikan instans Amazon EC2. Pilih instans dengan nama LabHost .
2. Di menu Status instans, pilih Hentikan instans. Pada jendela Hentikan instans, pilih Hentikan. Instans akan memasuki status berhenti dan akan mati.







1. Tutup jendela browser pribadi Anda.
2. Pilih Akhiri Lab di bagian atas halaman ini, lalu pilih Ya untuk mengonfirmasi bahwa Anda ingin mengakhiri lab. Pilih X di sudut kanan atas untuk menutup panel.

Menjelajahi pengguna dan grup IAM yang telah dibuat sebelumnya

Memeriksa kebijakan IAM sebagaimana diterapkan pada grup yang telah dibuat sebelumnya

Mengikuti skenario dunia nyata, menambahkan pengguna ke grup dengan kemampuan tertentu diaktifkan

Menemukan dan menggunakan URL masuk IAM

Bereksperimen dengan efek kebijakan pada akses layanan