AWS Organizations & IAM Identity Center (SSO)

Tuesday, September 10, 2024 9:05 AM

Today's Takeaways

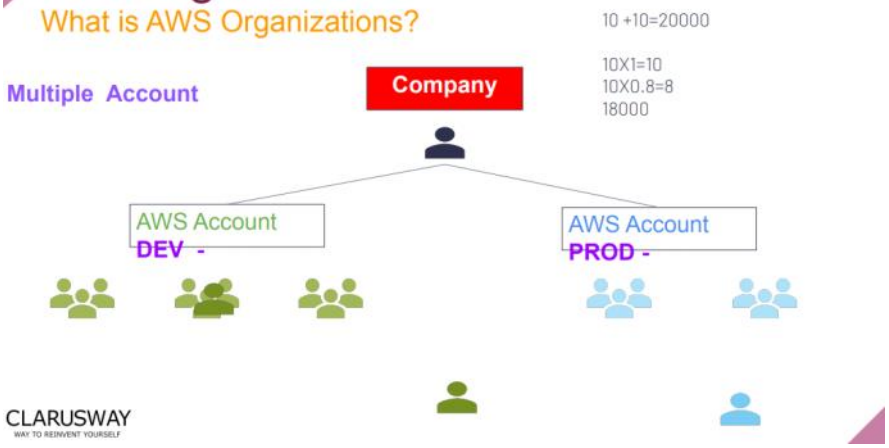
- Part 1 -AWS Organizations
- Part 2 -IAM - IAM Identity Center (SSO)
- Part 3 -Hands on

AWS Organizations

Bir AWS accountu var. bu accountun icerisinde gruplar var. credentiallari tek tek tayin etmek yerine gruplara bolup gruplara tayin etmek daha kolay. Haricinde kismak istedigimiz rolleri de kisi bazinda ayarlayabiliyorduk.
Burada teml mevzu account ve userlar.

AWS Organizations

What is AWS Organizations?



Senayo su ki bir company var. Burada iki tane AWS account acilmis. Development ve production kismi birbirine hic karismasin ayri ayri olsun diye boyle tercuh eden sirktler var.
Bu sekilde multiple accountlar oldugunda bir takim ihtiyaclar oluyor. Iste bu ihtiyaclari karsilamk icin AWS organizasyonu kullaniyoruz.

AWS Organizations

What is AWS Organizations?

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

AWS Organizations

AWS organizations bir mangement servis.
Multiple accountlari considible edebilmek icin yani onlarla ilgili kullanabilecek seyleri bir araya getirip onlardan maksimum faydayi saglayabilmek icin kullanilan bir yontem.
Birden fazla acoount uzerinde yetkileri kisitlamak veya arttirmak gerekebilir.
Bu accountlar uzerinde hem ekonomi hem management yonunde benefitleri gozeterek hareket etmek isteyebilirsiniz. O noktada da bunu kullanabiliriz.

AWS Organizations

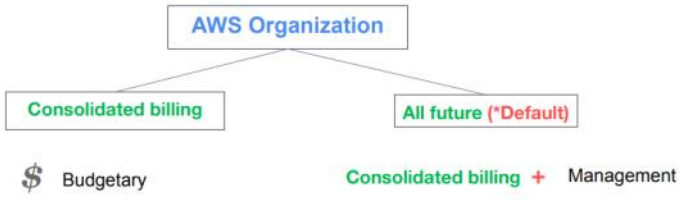
Features of AWS Organizations

- Centralized management of all of your AWS accounts
- Consolidated billing for all member accounts
- Hierarchical grouping of your accounts to meet your budgetary, security, or compliance needs (OUs)
- Policies to centralize control
- Integration with IAM and IAM Identity Center (SSO)

AWS organization birden fazla accountu tek bir yerden manage yapabiliyor. Bunlar uzerinde kurallar koyup tek bir noktadan yonetimini saglayabiliyorsun.
Diger en onemli husus consolidated billing mevzusu. Birden fazla hesabin daha az parayla optimizasyonunu saglar.
Hiyerarsik accountlar acip onlarin altinda yine farkli gruplandirmalar da yapabiliyoruz.
Bir agacin dallari gibi Ous(Organization Uniqs) denilen virtual gruplar da olusturuyoruz.
Bunlarin herbirisine nested 5 tane daha Ous kurabiliyoruz. Ous dedigimiz organizasyonlar arsindaki sanal mantiksal gruplardir.
Policylerle centralize ediyoruz.
IAM ile entegre edip daha degisik bir user tanimlama modeli karsimiza cikiyor(SSO). Bu bize ayni zamanda identity centeri daha efektiv kullanabilmeyi saglar.

AWS Organizations

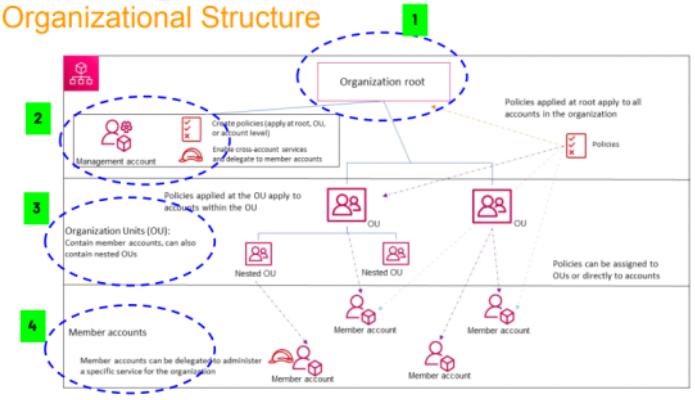
AWS Organizations Feature Sets



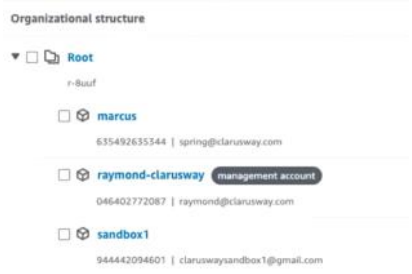
AWS organization iki amacla yapilan birsey. SINAVDA KARSIMIZA CIKABILIR!!!!
Bunlardan birisi consolidated billing digeri All future.
Consolidated billing dedigimiz sey tamamen addi cikarlar dogrultusunda hazirlanan bir organizasyon. Buradaki amac policyler vs degil tamamiyle fiyatlari nasil asagiya cekeriz, nasil tasarruf saglariz vs gibi budgetary isleri.
All future ise hem consolidated billling hem mangement kismi yani adi ustunde tum hersey. Yani hem butce kisimi hem de bu isi policylerle yoenetebilme kismi.
Bu durumda ne olmus oluyor? Senin olusturdugun o organizasyonun icine policy atayabilme yetkisi konulmus oluyor.

AWS Organizations

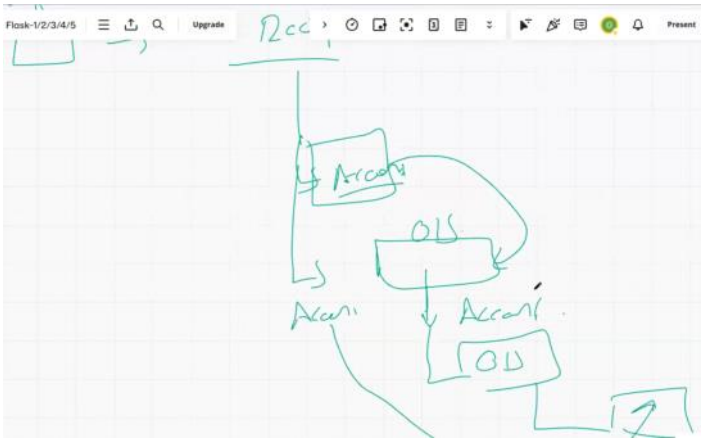
Organizational Structure



Olayin yonetimsel kisminda soyle birsey oluyor:
Biz organizasyon diye birsey enable ettigiimiz taktirde root diye birsey ortaya cikiyor. Tek hesap oldugunu dusunelim. Bu durumda direkt senin hesabina baglaniyor. Burda mesela rymond organizasyonu kuran. Kendi hesabindan bir organizasyon olustuyor. Ve hesabi enable ettigi an root altinda boyle bir goruntu ortay cikiyor.



Management accountun altina Ous kurabiliyoruz. Yani logic olrak birbirine daha yakin oldugunuz noktalari bir grup altinda toplayabiliyoruz. Hem OUs kurup hem account acabiliyorum.



Bu sekilde nested gruplar OUs olusturabiliyoruz.
Root altinda account da olabilir organization da olabilir.
OUs icinde account da olabilir yine bir baska OUs da olabilir. Ta ki 5 tane ic ice oluncaya kadar.
Bu Ous neden yapiyorum? Cunku aslinda bunlar grup olayina benziyor. Bunlara policy atayabiliyorum.
Boylece bu Ouslar icinde su kurallar uygulansin diye policyler atamis ve duzen saglamis oluyorum.
Ana kurucu management account digerleri member account diye geciyor.

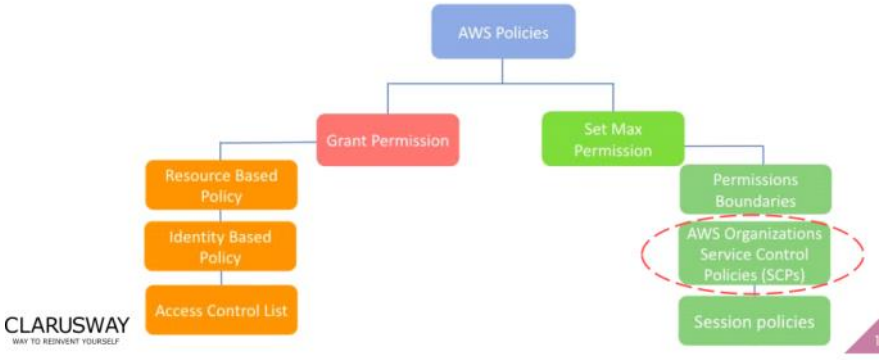
AWS Organizations
Supported Policy Types

- AI services opt-out Policies
- Backup Policies
- Service Control Policies*
- Tag Policies*

* will be practiced in hands-on

4 tip policy var az once bahsettigimiz Ous yonettigimiz ya da accountlari yonettigimiz.
Backup policy backup alma stratejilerini belirledigim buna gore butun hesaplarla ortak backup saglama sureci saglayabilecegim bir policy. AI icinde ayni sey gecerli.

AWS Organizations
Recap IAM Policy Types



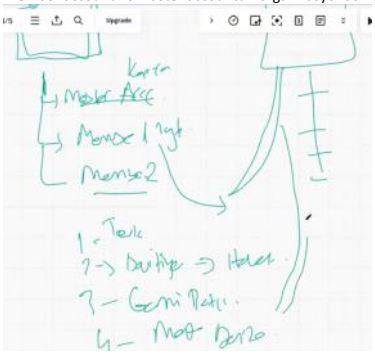
Grant permission aabanin motoru gibiydi. Belirli bir gucu vardi, hiz kesip hiz arttimayla iligleniyordu.
Set max permission ise hiz tabelalri. Yani bir kural var motor gucu kac olursa olsun o kurala gore hiz belirlemen gerek. Ote yandanda mesela hiz siniri 400 olsa haci murala 400 lle suremzsin kural o oldugu halde. Bir yapabilirligin var yani.
Set max permission tirpanlama uzerine, grant permission verme alma yetkisi.
AWS Organizations Service Control Policies ise set max permissions altinda.

AWS Organizations
AWS Organizations Exam Tip

Moving to Another Organization for the Member and Master Account

1. Remove the member account from the old Organization.
2. Send an invite to the member account from the new Organization.
3. Accept the invite to the new Organization from the member account.
4. Delete the old Organization.
5. Send an invite to the master account
6. Accept the invite to the new Organization from the master account

SINAVDA CIKAN BIR SORU UZERINE TIPS!!!!!!!
Member account ve master accountun organizasyondan ayrilma ile ilgili proedurleri var.



Iki ayri account var. bir accounttkiler diger accounta dagitilacak. Master en son terk ediyor. Diger memberlar once terk sonra diger ccounttan istek ve daha sonra kayit.
Ama master artik en son terk ettiginde eski accountu diger accounta member account olarak gecmis oluyor. Artik master degil.

AWS Organizations

AWS Organizations Pricing

- It is free to use AWS Organizations. AWS Organizations is offered at no additional charge.
- You are charged only for AWS resources that users and roles in your member accounts use.

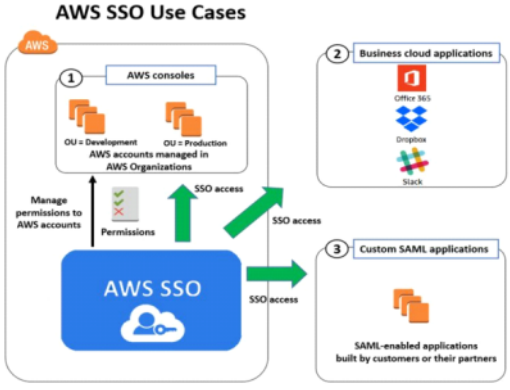
Bedava.
Sadece servislerden hangisini kullaniyorsa onlarin fiyatini oduyorsun.

IAM Identity Center (SSO)

IAM Identity Center (SSO)

What is IAM Identity Center?

AWS IAM Identity Center (successor to AWS Single Sign-On) is a service that makes it easy for you to centrally manage IAM Identity Center access to multiple AWS accounts and business applications.



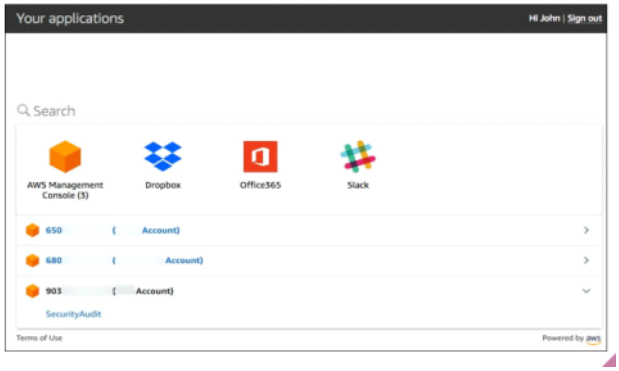
CLARUSWAY
WAY TO REINVENT YOURSELF

Single sign on diye gecer. Multiple accountlrda ve business applicationlarinda kullanilan bir yontem.

IAM Identity Center (SSO)

Key Features-IAM Identity Center user portal

In the user portal, you can find applications and AWS accounts which you have granted them access.



CLARUSWAY

Aslinda bizim nihai olarak ulasabilecegimiz boyle bir konsol oluyor.
burada vars bir veya birden fazla hesabi onu buradan bu sekilde gormus oluyoruz.
Varsa kullanidigi applikasyonlari onu da bu sekilde bunun uzerinden gormus oluyoruz.
Buyuk firmalarda zaten IAM ve root girisleri hic olmuyor. Direkt bu sekilde applikasyonlarina baglaniyorlr.
Sik kullanilan bir yontem olmaya basladi. Roleler IAM ler vs de ataniyor ama bu sistem dah cok tercih edilmeye bslandi.

IAM Identity Center (SSO)

Key Features- Integration with AWS Organizations

Tek konsol uzerinden birden fazla hesap uzerinden farkli yetkilere sahip olarak girebiliyorum.
Bu Single sign on olayinin guzelligi.
Bir kisi teker teker IAM user ile hesaplara girecegine tek bir hesapla rolleri yonetebiliyor.

AWS IAM Identity Center is integrated with Organizations to enable you to manage access to multiple AWS accounts in your organization.

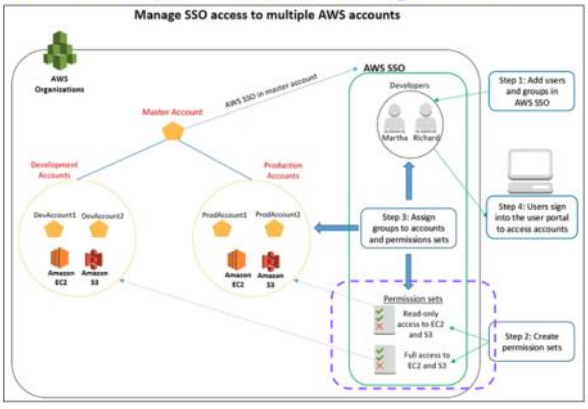
CLARUSWAY
WAY TO REINVENT YOURSELF

IAM Identity Center (SSO)

Key Features- Centralized permissions management

Master account altinda development account ve production account olarak iki account tanimlanmis. Burada developer grubuna su yetki verilmis: permission setlerle production kisminda sadece read yapabilsin, digerinde full acccess ec2 ve s3.

You can centrally manage the permissions granted to users when they access AWS accounts via the AWS Management Console.



IAM Identity Center (SSO)

Pricing

Kullandigin kadar ode.

- IAM Identity Center is offered at no extra charge.

AWS Organizations

Service Control Policies (SCPs)