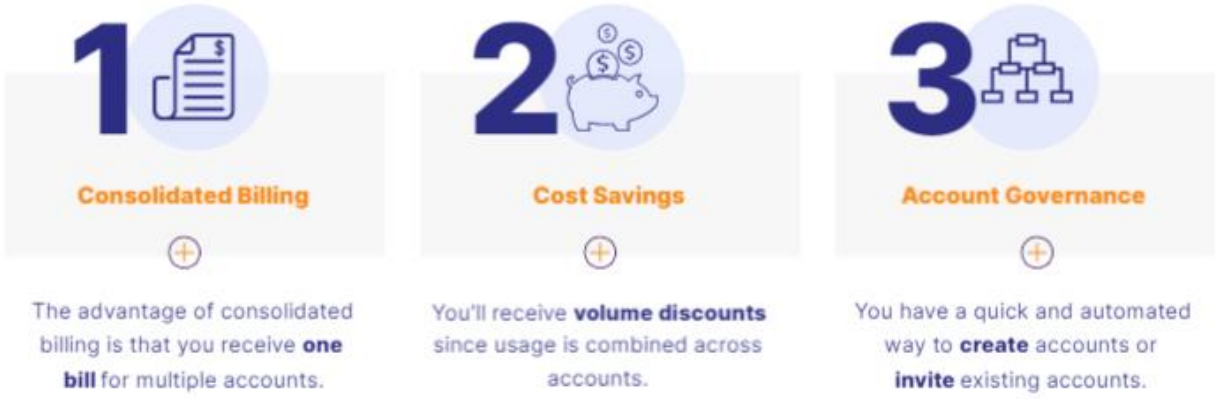
Governance

>Organizations

- Organizations
  - Formerly known as Consolidated Billing, AWS Organizations allows you to centralize the administration of multiple AWS accounts owned or controlled by a single company. This can make a lot of sense, since many companies will own more than one account—or might share AWS resources with vendors and clients. Being able to control the allocation of resource permissions, security, and spending from a single pane of glass is a big deal. It's also a convenient way to manage payments.
  - AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources.
  - Apply policies to accounts or groups for governance and simplify billing by using a single payment method for all your accounts.
  - Service Control Policies (Set limits on users permissions)
- Benefits of organizations



It is best practice to create a specific account dedicated to logging. CloudTrail supports logs aggregation.

>Sharing AWS RAM

AWS resource access manager (RAM) is a free service that allows you to share AWS resources with other accounts within your organization.

https://aws.amazon.com/ram/

Things we can share

1. Transit gateways
   a. Meaning we don't have to set one up in ever single account
2. VPC Subnets
   a. So we don't have to rebuild in every single account
3. License Manager
   a. Don't have to duplicate these
4. Many more…

^ You may see a trend “don’t have to”… This saves the time to continuously copy and paste and spend extra money in many environments when we could just have 1 location.

>Cross-Account Role Access

This is very important for the exam and the real world. This stops you from having to duplicate credentials multiple times. You can just have 1 primary AWS account to manage your sign-ins. And then from there, have users just assume roles. Examples could be like assuming a role to going into the Dev account, hop in the production account… etc.

Since you don’t have multiple sets of credentials out there, this helps with any security vulnerabilities.

Steps to set this up

1. Create an IAM Role
2. Set permissions
3. Grant access to that role
4. User then test the access
    a. by temporarily assume those sets of creds to be able to work in whatever they are going in.

Nobody else can assume this role besides the ones we allowed.

Role access needs to be given out, it's not there by default.

> Inventory Management with AWS config

- Config - Allows you to access, audit, and evaluate the configs of your resources.
    - Inventory Management and control

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

3 beneficial things for config

1. Allows us to query our resources
    a. Helps you discover what you have inside the environment
    b. Like what if you accidently deleted something and you don’t know what was deleted, how many instances you have
2. Rules to enforce what is happening
    a. These rules can be created to flag when something is going wrong
3. Learn the history of the environment
    a. Helpful when it comes to troubleshooting
    b. Hop into Config when things happened when a call was made, a change was made, better track down the issue so the issue can be resolved

> Offloading Active Directory of Directory Service

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft Active Directory (AD), enables your directory-aware workloads and AWS resources to use managed Active Directory (AD) in AWS.

- You don't want to have this on prem or anywhere else

This helps with SSO, group policy, and what makes things easier… AWS Directory service allows you connect to an already existing on-prem AD.

- Managed Microsoft AD
  - AWS Managed Microsoft AD provides you the option to administer your on-premises users, groups, applications, and systems without the complexity of running and maintaining an on-premises, highly available AD.
  - You can easily join your existing computers, laptops, and printers to an AWS Managed Microsoft AD domain.
- AD Connector
  - Creates a tunnel between AWS and your on-premises AD
  - That means that you get an endpoint that you can authenticate against inside of AWS… While leaving all of your actual users in data on-prem
- Simple AD
  - Basic AD service that is up and running inside of AWS
  - Powered by Linux Samba Active Directory compatible server

>Exploring with Cost Explorer

- Cost Explorer
  - Cost Explorer https://aws.amazon.com/aws-cost-management/aws-cost-explorer lets you build graphs to visualize your account's historical and current costs. If you're in a hurry, you can select one of the preconfigured views provided by the service (including spending over the most recent three months by service).
  - View past 12 months
  - If you are considering your options for Savings Plans, AWS Cost Explorer can analyze your EC2 usage over the past 7, 30, or 60 days.
  - Lets you build reports

We budget for obvious reasons… Money

We can easily break down cost on a service-by-service basis. Which also helps with next months billing which could predict the cost.

>AWS Budgets

AWS Budgets

- This allows you to set custom budgets that alert you when your cost or usage exceeds your budgeted amount.

- An AWS budget is a tool for tracking a specified set of events so that when a preset threshold is approached or passed, an alert—perhaps an email—is triggered.
- AWS budgets can be configured to send alerts when your resource consumption approaches or passes a preset limit.
- Track your cost, usage, or coverage and utilization for your Reserved Instances and Savings Plans, across multiple dimensions, such as service, or Cost Categories.

- Budget Types (4 types)
  - Cost Budgets
    - Plan on how much you want to spend on a service
  - Usage Budgets
    - Plan on how much you want to use on one or more services
  - Reservation Budgets
    - Set RIs or savings plans utilization or coverage targets
  - Savings Plans Budgets
    - Based on what you're doing is it covered by the savings plan

>Trusted Advisor

- Trusted Advisor
  - You use Trusted Advisor to visually confirm whether your account resource configurations are sound and are compliant with best practices.
  - Provides real-time guidance to help you provision your resources allowing AWS best practices

Trusted Advisor has 5 categories

Category	Purpose	Examples
1. Cost Optimization	Identifies any resources that are running and costing you money but are either underutilized or inactive	EC2 instances or Redshift clusters that, over time, are mostly idle
2. Performance	Identifies configuration settings that might be blocking performance improvements	Inappropriate reliance on slower magnetic or low throughput Elastic Block Store (EBS) volumes
3. Security	Identifies any failures to use security best-practice configurations	Simple Storage Service (S3) buckets with publicly accessible permissions or security groups permitting unrestricted access
4. Fault Tolerance	Identifies any running resources that, through poor configuration, are unnecessarily vulnerable to service disruptions	Data volumes that aren't properly backed up or instances that aren't replicated

5. Service Limits	Identifies resource usage that's approaching AWS Region or service limits (as described in Chapter 2, "Understanding your AWS Account")	Your account is currently using close to the 100 Simple Storage Service (S3) buckets limit

Exam Tips

1. Organizations
    a. May be given some scenarios to ensure that logs are centralized in one account to where nobody can't edit or delete the logs – Think organizations and use SCPs to restrict anyone from make changes to those logs
    b. SCPs are the best way to have the final say (Even restricts the root account)
    c. Billing can go into a single account for payment
    d. Sharing RIs an be shared across accounts (You can turn this off, but not best practice)
2. RAM | VPC Peering
    a. Sharing resources within the same region = RAM
    b. Sharing across regions = Use VPC Peering
        i. May see more questions on VPC peering than RAM.
    c. Sharing resources means saving money since you don't have to duplicate them
    d. VPC peering excels when connecting 2 separate networks
    e. RAM is free… But the user creating the architecture pays
    f. Organizations – RAM easily allows organizations to share architecture.
3. Cross-Account Role Access
    a. Anything about security, credentials… think of roles
    b. Use roles EVERYWHERE. Important piece for the exam
    c. Auditing
        i. Any temp employees get role access. NO permanent creds (Think Audit)
    d. Roles are temporary. You can't permanently assume a role
4. Inventory Management with AWS config
    a. Anything on the exam talking about enforcing standards thing Config.
    b. We can setup rules, and automatic remediation to fix those problems
    c. Config helps with things making sure things are lets say we have buckets and they a public but suppose to be private it will automate to be private. Make sure things stay encrypted
    d. Config is the best way to check that standards are applied to the architecture
    e. Deleted resources can be tracked using Config
    f. Use automation documents or Lambda to enforce your standards
        i. Both are on the exams according to the instructor
    g. Consolidate all your findings and rules into a single region
5. Offloading Active Directory of Directory Service
    a. Know the 3 types of Directory services : Managed Microsoft AD, simple AD and Connector
        i. A deep understanding of AD is not required on the exam… But it would be good to know about it.
    b. Fully managed service so when possible use the directory service over EC2 instanced for AD
        i. Favor using managed services over unmanaged services
    c. If a customer doesn't feel comfortable moving their users to the cloud, that is okay. As that is when AD Connector comes into play.
6. Cost Explorer

    a. Know when questions talk about budgeting or control spending. Think of Cost Explorer
    b. Remember you must set the tag as a cost allocation tag
    c. Cost Explorer and Budgets go hand in hand
        i. Which the cost explorer helps create a budget for your dept, team or individual
    d. Cost Explorer can estimate your upcoming monthly cost.
    e.
7. AWS Budgets
    a. Current spend or projected spend can be alerted to users
    b. Budgets are the best way to let users know they're getting close to overspending
    c. Use Cost Explorer to create fine-grained budgets (Good experience to have for employment)
        i. You can also use cost explorer to create very specific budgets)
    d. Be proactive, once the money is gone, it is gone
    e. Tags can be used to create very specific budgets
8. Trusted Advisor
    a. Focus on answers that have an automated solution
    b. Something is wrong? Tell someone!
    c. Trusted Advisor will not fix the problems for you
    d. Use EventBridge to kick off Lambda to solve the problem for you