
aws
certified
Solutions
Architect
Professional
DOLFINed

DESIGNING FOR ORGANIZATIONAL COMPLEXITY AND COST MANAGEMENT/CONTROL

You Can Do It Too!

AWS Cost Management

AWS Cost Explorer & AWS Budgets

AWS Cost Explorer

- A free service provided by AWS which can be used for:
  - Viewing the AWS cost data as a graph.
  - Filter graphs by values such as API operation, Availability Zone, AWS service, custom cost allocation tag, Amazon EC2 instance type, purchase option, region, usage type, usage type group, and more.
  - When using consolidated billing, you can also filter by member account.
  - In addition, you can see a forecast of future costs based on your historical cost data.

AWS Budgets

- AWS Budgets enable AWS clients to plan their service usage, service costs, and instance reservations.
- Budgets provide AWS clients with a way to see the following information:
  - How close the plan is to the budgeted amount or to the free tier limits
  - The account(s) usage to date, including how much have been used of the Reserved Instances (RIs)
  - The current estimated charges from AWS and how much the predicted usage will incur in charges by the end of the month
  - How much of the set budget has been used
- Budgets use the cost visualization provided by AWS Cost Explorer to show the status of an account's budgets,
- Budgets can be used to create Amazon SNS notifications that sends notifications:
  - When the usage goes over the budgeted amounts, or
  - When the estimated (forecasted) costs exceed the configured budgets.

AWS Budgets - Types

- The following types of budgets can be created:
  - **Cost budgets** – Plan how much is desired to spend on a service.
  - **Usage budgets** – Plan how much is desired to use on one or more services.
  - **RI utilization budgets** – Define a utilization threshold and receive alerts when the RI usage falls below that threshold.
    - This shows whether the RIs are unused or under-utilized.
  - **RI coverage budgets** – Define a coverage threshold and receive alerts when the number of instance hours that are covered by RIs fall below that threshold.
    - This allows the visibility into how much of instance usage is covered by a reservation.

AWS Budgets and AWS Organizations

- Single accounts and master and member accounts in an AWS Organizations organization can, by default, create budgets.
- When you create a budget, AWS Budgets provides a Cost Explorer graph to help visualize the incurred costs and usage.
- Optional notifications (sent to SNS topic, email, or both) can be setup to warn if:
  - The budgets, or the forecasted usage is to exceed the amount budgeted for cost or usage.
  - If the usage falls below the budgeted amount for RI budgets

AWS Cost Management

Consolidated Billing

AWS Organizations (Consolidated Billing)

- If you use consolidated billing in an organization and you own the master account, you can use IAM policies to control access to budgets by member accounts.
- By default, owners of member accounts can create their own budgets but can't create or edit budgets for other users.
- You can use IAM to allow users in a member account to create, edit, delete, or read the budget for your master account.
  - Do this, for example, to allow another account to administer your budget.

- In an organization, the master account is responsible for paying all charges that the member accounts incur.
- An administrator of a master account that has the appropriate permissions, can view aggregated usage costs for Reserved Instance discounts and volume tiering for all member accounts.
  - This administrator can also view the charges that individual member accounts incur,

Consolidating Billing – Master Account and Charges

- Like member accounts, a master account can incur usage charges.

- AWS best practices calls for avoiding using the master account to run AWS services.
  - This is not including the services and resources that are required to manage the organization itself. Like the S3 bucket(s) in the master account, where AWS cost and usage reports will be saved.

Consolidated Billing (Multiple Accounts) vs One Account/ Multiple VPCs

- Consolidated Billing:
  - Easier from an AWS architecture perspective
  - Volume discounts
  - Primarily relies on IAM roles and attached permissions for cross account access
  - Complex tagging cross accounts

- One Account – Multiple VPCS
  - Simple billing, one bill for one account
  - Easier governance, single account
  - No need for IAM roles cross-account
  - Tagging is easier at a single account level
  - More complex setup to allow for resource level permissions
  - More complexity in setting up the VPCs

Consolidated Billing for Organizations – Reserved Instances

- For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account.
  - This means that all accounts in the organization can receive the hourly cost benefit of Reserved Instances that are purchased by any other account.

- The payer account of an organization can turn off Reserved Instance (RI) sharing for any accounts in that organization, including the payer account.
  - This means that Reserved Instances aren't shared between any accounts that have sharing turned off.
  - To share an RI with an account, both accounts must have sharing turned on.

- You can turn off Reserved Instance sharing on the **Preferences** page on the Billing and Cost Management console.

AWS Cost Management

Notification and Alerts Scenarios

Monitoring Charges with Alerts and Notifications

- AWS costs can be monitored using CloudWatch.

- With CloudWatch, billing alerts can be created to send notifications when the usage of services exceeds the defined thresholds,
  - These threshold amounts can be specified when creating the billing alerts.
  - When the usage exceeds these amounts, AWS sends an email notification.
  - Notifications also can be sent (if signed up for it) when AWS prices change.

AWS Cost Management

Resource Groups & Cost Allocation Tags

Cost Allocation Tags

- A tag is a label that you or AWS assigns to an AWS resource.
  - Each tag consists of a *key* and a *value*. A key can have more than one value.
- Tags can be used to organize your resources, and cost allocation tags to track the AWS costs on a detailed level.
- After activating cost allocation tags, AWS uses the cost allocation tags to organize the resource costs on the cost allocation report, to make it easier to categorize and track the AWS usage costs.
- AWS provides two types of cost allocation tags,
  - An *AWS generated tags, where* AWS defines, creates, and applies the AWS generated tags, and
  - User-defined tags where Users/Clients define, create, and apply user-defined tags.
- Only master accounts in an organization and single accounts that are not members of an organization have access to the **Cost Allocation Tags** manager in the Billing console.

Resource Groups

- AWS Resource group, is a number of AWS resources sharing one or more tags

AWS Cost Management

Cost Optimization Considerations

Cost Optimization on AWS

The right EC2 Instance Sizing

- In some cases, selecting the cheapest type that suits workload's requirements might be the best.
- In other cases, using larger instance type can help reduce the overall cost for better performance.
- The use of benchmarking to select the right instance type which depends primarily on how the workload utilizes CPU, RAM, network, storage size, and I/O.
- Cost can also be reduced by selecting the right storage solution for the needs.
  - For example, S3 offers a variety of storage classes, that differ in cost, but also in the features they provide.
  - Other services, such as EC2, RDS, and ES support different Amazon EBS volume types (general purpose SSD, provisioned IOPS SSD,….etc) that should be evaluate based on the requirements.

Cost Optimization on AWS & Tagging

Continuous monitoring and tagging

- Cost optimization is an iterative process. The applications on AWS and their usage will evolve through time.
  - Moreover, AWS iterates frequently and regularly releases new options.

Tagging Strategies on AWS

- Tagging can be made a part of your build process and automate it with AWS management tools like AWS Elastic Beanstalk and AWS OpsWorks.

- The managed rules provided by AWS Config can be used to assess whether specific tags are applied to your resources or not.

AWS Cost Management

Cost Optimization Considerations

EC2 Purchasing Options

Amazon EC2 provides the following purchasing options to enable you to optimize your costs based on your needs:

- **On-Demand Instances** – Pay, by the second, for the instances that you launch.
- **Reserved Instances** – Purchase, at a significant discount, instances that are always available, for a term from one to three years.
- **Scheduled Instances** – Purchase instances that are always available on the specified recurring schedule, for a one-year term.
- **Spot Instances** – Request unused EC2 instances, which can lower your Amazon EC2 costs significantly.
- **Dedicated Hosts** – Pay for a physical host that is fully dedicated to running your instances, and bring your existing per-socket, per-core, or per-VM software licenses to reduce costs.
- **Dedicated Instances** – Pay, by the hour, for instances that run on single-tenant hardware.
- **Capacity Reservations** – Reserve capacity for your EC2 instances in a specific Availability Zone for any duration.

Purchasing Options – Reserved Instances

RI best practice:

- You should not commit to Reserved Instance purchases before sufficiently benchmarking your application in production. After you have purchased reserved capacity, you can use the Reserved Instance *utilization reports to ensure you are still making the most of your reserved capacity.*

RI Attributes:

- **Instance type**: For example, m4.large. Instance family/size
- **Scope**: Zonal (AZ) or Regional (Region RI)
- **Tenancy**: The RI instance runs on shared (default) or single-tenant (dedicated) hardware.
- **Platform**: Linux or Windows

Purchasing Options – Reserved Instances Types (Offering Classes)

- If your computing needs change, you may be able to modify or exchange your Reserved Instance, depending on the offering class. Offering classes may also have additional restrictions or limitations.

- **Standard RI: (can be zonal or regional)**
  - You can not change the instance type during the term
  - You can change instance size

- **Convertible RI: (can be zonal or regional)**
  - Can be exchanged during the term for another Convertible Reserved Instance with new attributes including instance family, instance type, platform, scope, or tenancy.

Purchasing Options – Scheduled (Reserved) Instances

- **Scheduled (Reserved) Instances** –
  - Purchase instances that are always available on the specified recurring schedule, for a one-year term.
  - Use when purchasing capacity reservations that recur on a daily, weekly, or monthly basis with a specified start time and duration.
  - You reserve the capacity in advance, so that you know it is available when you need it.
  - You pay for the time that the instances are scheduled, even if you do not use them.

Purchasing Options – Spot Instances Strategies

- You can also use Spot Instances when you require more predictable availability:
- **Mix with On-Demand:**
  - Consider mixing Reserved, On-Demand, and Spot Instances to combine a predictable minimum capacity with "opportunistic" access to additional compute resources depending on the spot market price.
- **Spot Blocks for Defined-Duration Workloads:**
  - You can also bid for fixed duration Spot Instances.
  - These have different hourly pricing but allow you to specify a duration requirement.
  - If your bid is accepted your instance will continue to run until you choose to terminate it, or until the specified duration has ended;
    - Your instance will not be terminated due to changes in the Spot price
  - Spot instances can be launched independently, with Auto Scaling, or EMR (task nodes)
  - Redshift does not use Spot Instances

Cost Optimization on AWS

Dedicated Hosts vs Dedicated Instances

	Dedicated Hosts	Dedicated Instances
Billing	Per host	Per Instance
Visibility at the core, socket, and host ID level	Yes	Not Supported
Host and Instance Affinity	Allows the deployment of instances on the same dedicated host	Not supported
Targeted Instance Placement	Yes, visibility is provided	Not Supported
Automatic Instance Recovery	Not Supported	Yes
BYOL	Yes	Not Supported

Cost Optimization on AWS – Purchasing Options

- **On-demand Capacity Reservations** –
  - You can use your Regional RIs with your Capacity Reservations to benefit from billing discounts.
    - This gives you the flexibility to selectively add capacity reservations and still get the Regional RI discounts for that usage.
    - AWS automatically applies your RI discount when the attributes of a Capacity Reservation match the attributes of an active Regional RI.

Cost Optimization on AWS – Purchasing Options

When to use what?

- Amazon EC2 On-Demand instance pricing gives you maximum flexibility with no long term commitments, use it when you want few hours per day usage, or on/off usage but require availability when you need it.

- If you require a **capacity reservation (guaranteed availability)**, purchase:
  - Reserved Instances or
  - Capacity Reservations for a specific Availability Zone, or
  - Purchase Scheduled Instances.

- Spot Instances are a cost-effective choice if you can be flexible about when your applications run and if they can be interrupted.

- Dedicated Hosts can help you address compliance requirements and reduce costs by using your existing server-bound software licenses.

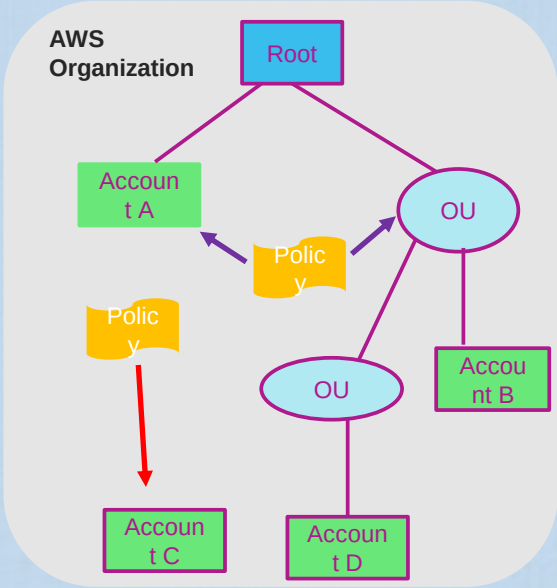
AWS ORGANIZATIONS

AWS Organizations

Introduction

What is it ?

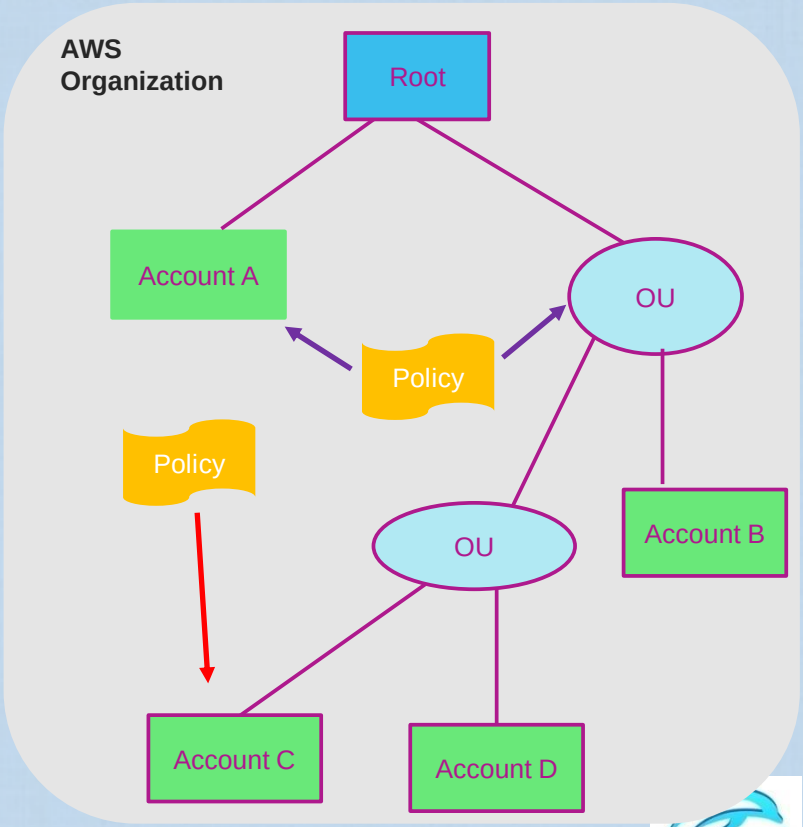
- AWS Organizations is a service for account management. It enables managing multiple AWS accounts at scale.
  - This is done by consolidating multiple AWS accounts into a single organization.
  - It also allows for centrally managing this organization from a master account
  - It includes consolidated billing capability, which enables customers to meet their financial control, budgetary, compliance, and security objectives while on AWS
- Consolidating accounts into a single organization simplifies how you use other AWS services.
- Administrators of AWS Organizations can include existing AWS accounts in an organization, or
  - Create new accounts to be part of an AWS Organization.
- AWS Organizations is free of charge
- It is a Global Service like IAM



Top down Organization tree - Components

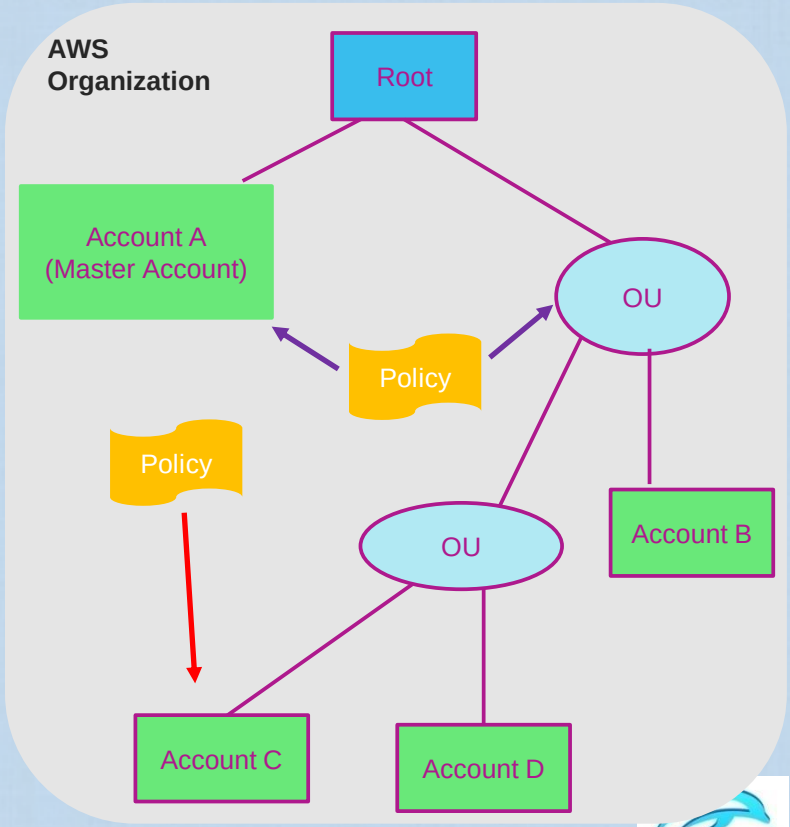
An AWS Organization has the following components:

- **Root**
  - Is the parent container of all accounts and organizational units (OUs) in the organization
    - A policy applied to the root flows down and becomes applied to all OUs and Accounts in the organization
    - Root is created automatically when you create the organization
    - Only one root in an organization (may change)
- **Organizational Units (OUs)**
  - An OU is a container of other OUs and accounts
  - An OU can have only one parent
  - An account can be a member of only one OU
  - Applying a policy at the OU level flows down to other OUs and Accounts under it



Top down Organization tree – Components (cont.)

- **Organizational Units (OUs) [can be nested]**
  - A policy that is applied to an account affects only that account
  - A policy that is applied at an OU flows down to all OUs and accounts under that OU
- **Accounts**
  - AWS Organization has a **Master Account**, which is the primary
  - All other accounts in the organization are called **Member accounts**
  - The master account is the **Payer account,** responsible for paying for all charges incurred by member accounts
  - An account can be a member of **only one** AWS organization at a time.
- IAM continues to be used at the account level to create:
  - Users , Roles, Permissions and policies
  - Create and manage Cross Account access permissions



AWS Organizations

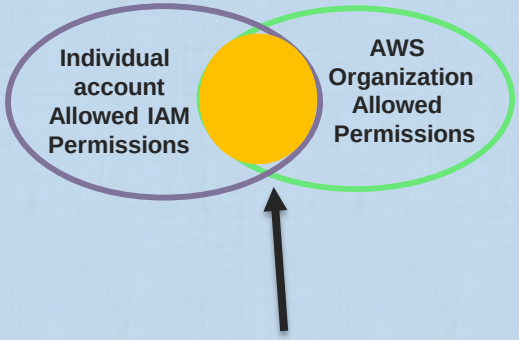
Features

Features

- **Centralized management of all the AWS accounts in the organization**
- **Consolidated Billing for accounts those are members in the organization**
- **Hierarchical grouping of AWS accounts to meet budgetary, security, or compliance needs**
  - You can group your accounts into organizational units (OUs) and attach different access policies to each OU.
- **Enables control over what AWS services and APIs each account (in the Org.) can access**
  - Organization permissions overrule account permissions.
  - The master account administrators have a higher control and authority over the administrators of the individual accounts in the AWS Organization
  - The master account administrators can restrict which AWS services and individual API actions the users and roles in each member account can access.
  - Such a restriction would overrides the administrators in the individual Oraganization's accounts

Features - Integration and support for AWS IAM

- When the master account Admins restrict access of a member account A, to a certain service or API,
- This overrides any account A administrators' explicitly granted permissions, by an IAM policy, to an IAM user or IAM Role to access that service or API.
- AWS Organizations provides for a granular level of control over what IAM users and Roles in individual accounts can do.
  - The user or Role can access only what is allowed by both the AWS Organizations policies and IAM policies.
    - If a privilege/action is denied by either one, the IAM user or Role can't perform that action (for example access to a service, or an API).



The intersection (overlap) Area represents the resulting Allowed permissions

Eventual Consistency and Data Replication in AWS Organizations

- AWS Organizations is highly available, this is achieved by replicating data across multiple servers in AWS data centers **within its region.**

- If configuration, policies or any AWS organization data is changed successfully, it will be committed and Stored.
  - However, the update to all the servers where the organization data is stored, however, will take some time to be replicated.

- Having said that, AWS Organizations is eventually consistent.

AWS Organizations

- Modes of Operation
- Service Control Policies (SCPs)

AWS Organizations Feature Sets..

AWS Organizations operates in one of two modes:

- **Consolidated billing:**
  - Only Consolidated billing features is used/enabled
  - It does not include the other advanced features of AWS Organizations

- **All Features:**
  - Includes the full feature set of AWS Organizations
  - Can be set for a newly created AWS Organization, or can be enabled from the consolidated billing mode
    - In case of enabling All features from the consolidated billing mode, an invitation is sent from the master account, to all member accounts, and they have to approve the change first.
    - The master account:
      - Has full control over what member accounts can do
      - Can apply Service Control Policies (SCPs) that can restrict what all IAM users (including root) and IAM Roles in the accounts can do or access.
      - Can prevent member accounts from leaving the organization

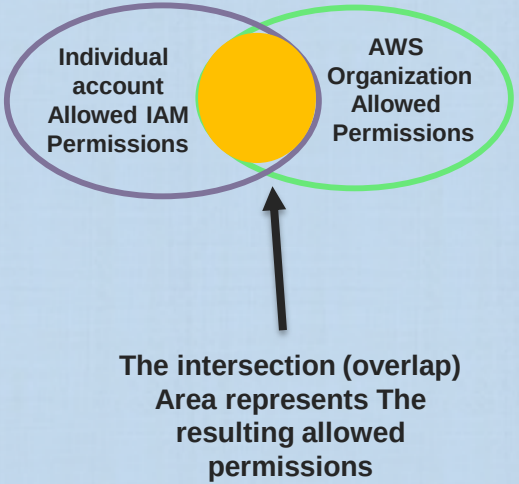
Service Control Policies (SCPs)

- A Service Control Policy (SCP) defines the services and actions that IAM users and IAM Roles can do, in the accounts, to which the SCP is applied to.

- An SCP does NOT grant permissions, however, it defines the maximum permissions that affected accounts (and IAM users or IAM Roles within those accounts) can have.

- SCPs can be applied at:
  - The AWS Organization's root,
    - This will affect all the accounts in the organization
  - An OU level, which will affect all accounts in the OU or any OU under the OU to which the SCP is applied
  - At an individual account level

- The SCPs has no effect on:
  - The master account, regardless whether the SCP was applied at the root, an OU where the master resides, or directly to it.
  - Any actions done using service-linked roles' attached permissions



Whitelisting and Blacklisting

- **Whitelisting:**
  - The policy specifies the list of access or actions that are allowed. All other actions and access will be implicitly blocked/denied.
  - By default, AWS organization's root, OUs, and accounts have a default policy applied by AWS Organizations, called **FullAWSAccess.**
    - Hence by default, AWS Organizations service does NOT block any access or actions in the OUs or accounts in the organization. In other words everything allowed by IAM is whitelisted
    - To change the default, you need to replace the default policy with the one that have the whitelisted actions or access
    - If you place the policy (non-default) at the root level, all the AWS organization will be affected by the restrictions imposed.
      - ➢ You can NOT add what is denied by the non-default policy applied at the organization's root, below the root, by allowing the denied permissions in different policies (applied below the root, at the OU or account level).
      - ➢ Remember, SCPs are not granting permissions, they are only filtering permissions.

Whitelisting and Blacklisting (cont.)

- **Blacklisting:**
  - Is the default for AWS Organizations
  - The policy specifies the list of access or actions that are denied. All other actions and access are allowed, unless explicitly blocked.
  - To establish this, leave the FullAWSAccess policy at the root, and attach more policies that define what is restricted/denied.
    - Like IAM, an explicit deny overrides any allow

AWS Organizations

AWS Services to use with Organizations

Integrating AWS Services with AWS Organizations

Integration with other AWS services

- AWS Organizations integrates with the following AWS services:
  - **CloudTrail :** Central logging of all the organizations' accounts logs
    - A user in a master account, with the proper permissions, can create an organization (Cloudtrail) trail that logs all events for all accounts in the organization.
  - **CloudWatch Events :**
    - Enable sharing of CloudWatch events across all the organization's accounts
  - **AWS Config:**
    - Obtain an Organization wide view of the compliance status of your resources' configurations in all accounts.
  - **Artifact:**
    - Allows for the download of compliance reports such as PCI and ISO for the organization.
  - **AWS Firewall Manager**
    - Centrally manage all WAF configurations across all accounts in your organization, from a central location
  - **AWS Directory Service**
    - The integration with Organizations Allows for, seamless directory service sharing across multiple accounts and any VPC in a Region.

Integrating AWS Services with AWS Organizations

- **AWS License Manager**
  - The integration allows for cross-account discovery of computing resources throughout the AWS organization, to ensure license compliance of the resources in the organization
- **AWS RAM**
  - Allows for sharing resources across accounts in your organizations (ex. Sharing Subnets, Transit gateway).
- **AWS Service Catalog**
  - Enables the sharing, and management of Products/Portfolios across the organization's accounts, from catalogs of IT services approved for use on AWS
- **AWS Single Sign-on**
  - Allows users to use AWS SSO to access their assigned accounts (master or member) using their corporate credentials.
- Please check the following link for the updated list
  - https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrated-services-list.html

Integrating AWS Services with AWS Organizations

- AWS Organizations creates an IAM service-linked role for the AWS service, in each member account of the AWS Organization, when that AWS service is configured/authorized to access your AWS Organization.
  - The created service-linked role will have the required policies and permissions, that are required to carry out only the configured/authorized tasks in the organization, and its accounts.

AWS Organizations

Best Practices

Best Practices

- Use AWS Cloutrail to monitor and log activities in the master account
- Do not add resources in the master account (except those are a must have)
- Use the least privilege principle
- Assign SCPs at the OU level instead of account level, easy scaling
- Test your SCPs first on an account before rolling out
- Avoid assigning SCPs at the root level, unless if absolutely necessary
- Use either Whitelisting or Blacklisting, but not both
- Establish a clear strategy as to when to create a new account