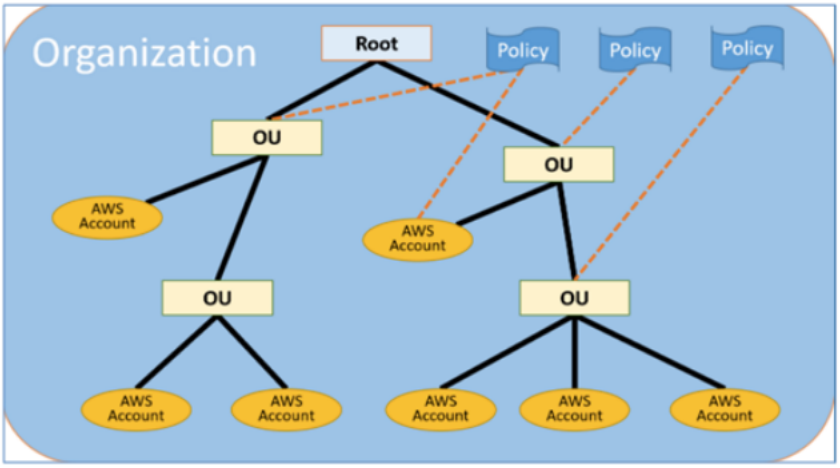
AWS - Organizations

- Using AWS Organizations and Service Control Policies to control services on each account is the correct answer.
- Refer to the diagram below:



Use AWS Organizations to centrally manage all of your accounts. Group your accounts, which belong to a specific business unit, to individual Organization Units (OU). Create an IAM Role in the production account which has a policy that allows access to the EC2 instances including a resource-level permission to terminate the instances owned by a particular business unit. Provide the cross-account access and the IAM policy to every member accounts of the OU.
(Correct)

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 includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business. As an administrator of an organization, you can create accounts in your organization and invite existing accounts to join the organization.

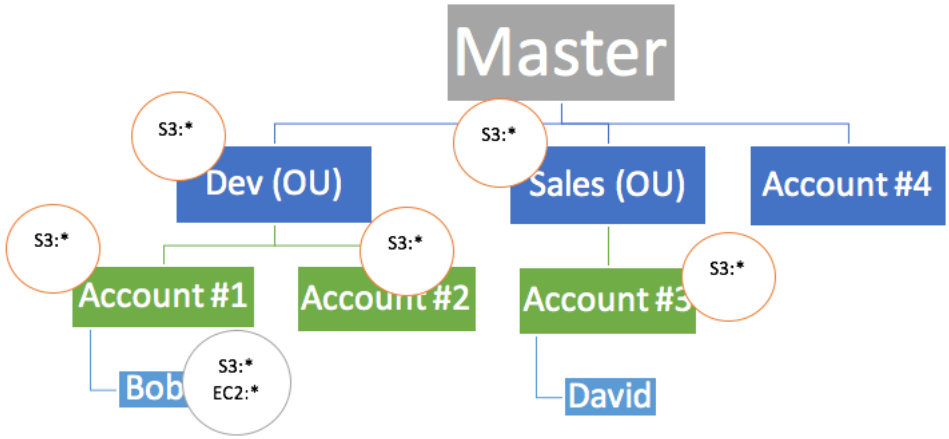
You can use organizational units (OUs) to group accounts together to administer as a single unit. This greatly simplifies the management of your accounts. For example, you can attach a policy-based control to an OU, and all accounts within the OU automatically inherit the policy. You can create multiple OUs within a single organization, and you can create OUs within other OUs. Each OU can contain multiple accounts, and you can move accounts from one OU to another. However, OU names must be unique within a parent OU or root.

Resource-level permissions refers to the ability to specify which resources users are allowed to perform actions on. Amazon EC2 has partial support for resource-level permissions. This means that for certain Amazon EC2 actions, you can control when users are allowed to use those actions based on conditions that have to be fulfilled, or specific resources that users are allowed to use. For example, you can grant users

permissions to launch instances, but only of a specific type, and only using a specific AMI.

SERVICE CONTROL POLICIES (SCP)

- AWS Organizations offers policy-based management for multiple AWS accounts.
- With Organizations, you can
  - create groups of accounts,
  - automate account creation,
  - apply and manage policies for those groups.
- Organizations enables you to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes.
- It allows you to create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts.
- Remember that AWS Organizations **does not** replace associating IAM policies with users, groups, and roles within an AWS account. Hence, you still need to set up appropriate IAM policies for your root and member accounts.



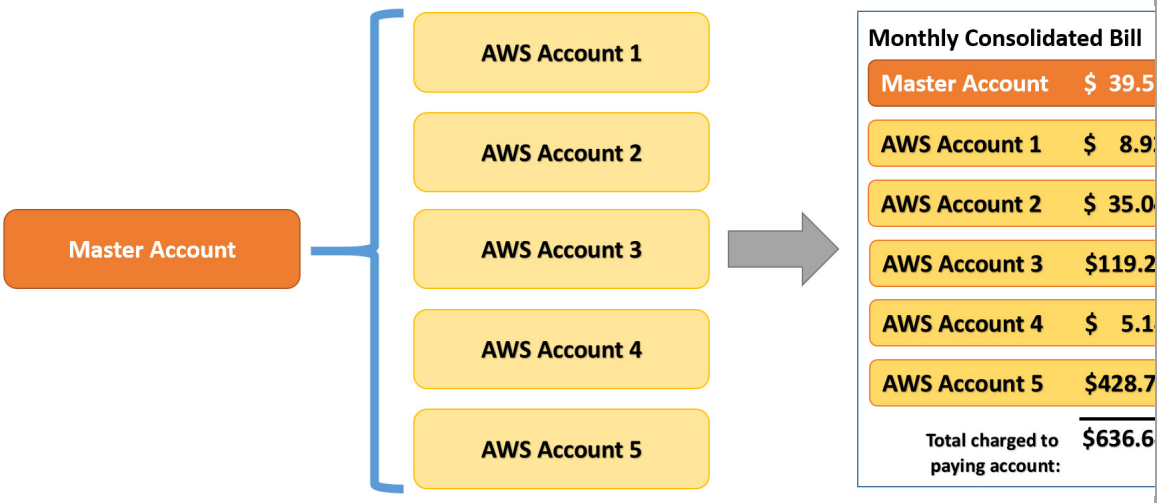
- IAM policies let you allow or deny access to AWS services (such as Amazon S3), individual AWS resources (such as a specific S3 bucket), or individual API actions (such as s3:CreateBucket). An IAM policy can be applied only to IAM users, groups, or roles, and it can never restrict the root identity of the AWS account.
- By contrast, AWS Organizations lets you use service control policies (SCPs) to allow or deny access to particular AWS services for individual AWS accounts, or for groups of accounts within an organizational unit (OU). The specified actions from an attached SCP affect all IAM users, groups, and roles for an account, including the root account identity.
- When you apply an SCP to an OU or an individual AWS account, you choose to either **enable** (whitelist), or **disable** (blacklist) the specified AWS service. Access to any service that isn't explicitly allowed by the SCPs associated with an account, its parent OUs, or the master account is **denied** to the AWS accounts or OUs associated with the

SCP. When an SCP is applied to an OU, it is inherited by all of the AWS accounts in that OU.

- **INCORRECT**
- **Setting up a common IAM policy that can be applied across all AWS accounts** is incorrect because it is not possible to create a common IAM policy for multiple AWS accounts.

CONSOLIDATED BILLING feature

- You can use the consolidated billing feature in AWS Organizations to consolidate payment for multiple AWS accounts or multiple AISPL accounts.
- With consolidated billing,
  - you can see a combined view of AWS charges incurred by all of your accounts.
  - You can also get a cost report for each member account that is associated with your master account.
- Consolidated billing is offered at no additional charge. AWS and AISPL accounts can't be consolidated together.



TAG based SCPs (control policies)

You can specify tags for EC2 instances and EBS volumes as part of the API call that creates the resources. Using this principle, you can require users to tag specific resources by applying conditions to their IAM policy.

Using AWS Organizations, you can consolidate all of your AWS accounts and group the business units into separate Organizational Units (OUs) with a custom service control policy (SCP).

Hence, the correct solution for this scenario is the option that says:

Configure AWS Organizations to group different accounts into separate Organizational Units (OU) depending on the business function. Create a Service Control Policy that

restricts launching any AWS resources without a tag by including the Condition element in the policy which uses the ForAllValues qualifier and the aws:TagKeys condition. This policy will require its principals to tag resources during creation. Apply the SCP to the OU which will automatically cascade the policy to individual member accounts.

You can configure your IAM policy to allow a user to launch an EC2 instance and create an EBS volume only if the user applies all the tags that are defined in the policy using the **ForAllValues** qualifier. If the user applies any tag that's not included in the policy then the action is denied. To enforce case sensitivity, use the condition ***aws:TagKeys***.

Here's a quick video on how to implement it in AWS:

https://youtu.be/qwMxh1x9UZQ

You can use organizational units (OUs) to group accounts together to administer as a single unit. This greatly simplifies the management of your accounts. For example, you can attach a policy-based control to an OU, and all accounts within the OU automatically inherit the policy. You can create multiple OUs within a single organization, and you can create OUs within other OUs.

AWS Organization with CloudWatch Events

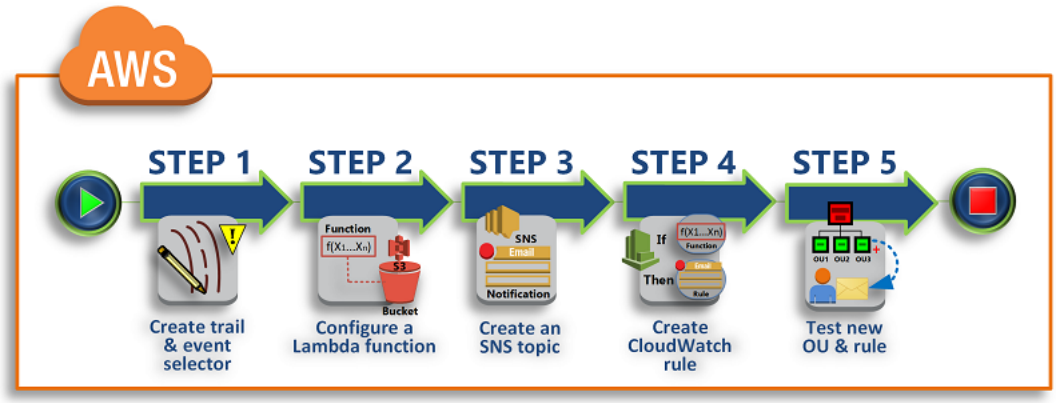
AWS Organizations can work with CloudWatch Events to raise events when administrator-specified actions occur in an organization. For example, because of the sensitivity of such actions, most administrators would want to be warned every time someone creates a new account in the organization or when an administrator of a member account attempts to leave the organization. You can configure CloudWatch Events rules that look for these actions and then send the generated events to administrator-defined targets. Targets can be an Amazon SNS topic that emails or text messages its subscribers. Combining this with Amazon CloudTrail, you can set an event to trigger whenever a matching API call is received.

Multi-account, multi-region data aggregation in AWS Config enables you to aggregate AWS Config data from multiple accounts and regions into a single account. Multi-account, multi-region data aggregation is useful for central IT administrators to monitor compliance for multiple AWS accounts in the enterprise. An aggregator is a new resource type in AWS Config that collects AWS Config data from multiple source accounts and regions

Hence, the following options are the correct answers in this scenario:

1. Create a trail in Amazon CloudTrail to capture all API calls to your AWS Organizations, including calls from the AWS Organizations console and from code calls to the AWS Organizations APIs. Use CloudWatch Events and SNS to raise events when administrator-specified actions occur in an organization and send a notification to you.

2. Use AWS Config to monitor the compliance of your AWS Organizations. Set up an SNS Topic or CloudWatch Events that will send alerts to you for any changes.



References:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_monitoring.html

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_tutorials_cwe.html

Reference:

https://aws.amazon.com/organizations/

Check out this AWS Organizations Cheat Sheet:

https://tutorialsdojo.com/aws-cheat-sheet-aws-organizations/

Service Control Policies (SCP) vs IAM Policies:

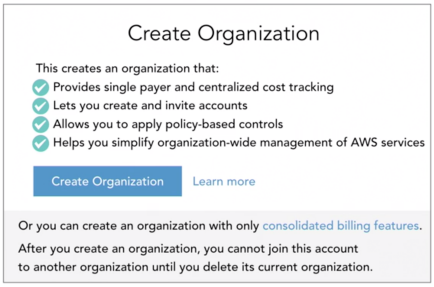
https://tutorialsdojo.com/aws-cheat-sheet-service-control-policies-scp-vs-iam-policies/

Comparison of AWS Services Cheat Sheets:

https://tutorialsdojo.com/comparison-of-aws-services-for-udemy-students/

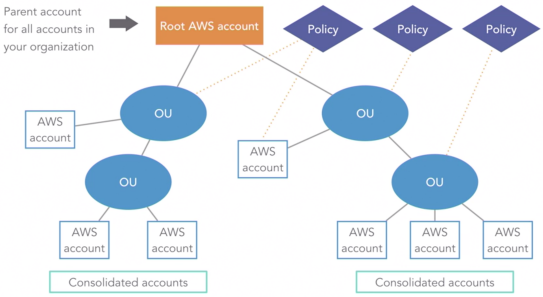
AWS Organizations	AWS Organization Features
• AWS account management service • Centrally apply security policy-based controls across multiple AWS accounts • Organize accounts into desired organizational unit (OU) structure	• Organizational permissions overrule individual AWS account permissions • Hierarchal grouping of multiple AWS accounts integrated with Identity and Access Management (IAM) control • Users can access only what is allowed by both organizational policies *and* IAM policies

Feature Sets



The master account is assigned the responsibility of the payer account.

It is responsible for paying all charges that are accrued by the member accounts.



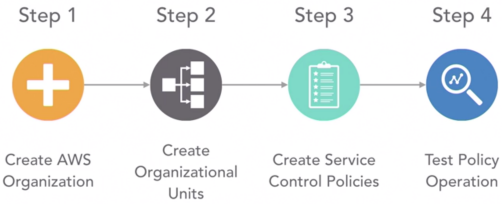
Service Control Policies (SCPs)

- Can be applied to a root account; affects all accounts in the AWS Organizations tree
- Can be applied to an OU; affects all accounts in that OU and all accounts that are contained within an OU subtree
- An individual AWS account

- A security filter that defines the services and actions that users and roles can use where the SCP is applied
- SCPs act like allow/deny filters
- Only the specified services and actions that are defined in both the SCP and IAM policy will be allowed or denied
- SCPs affect only principals that are managed by AWS accounts that are part of AWS Organizations

- SCPs work with Identity and Access Management (IAM)
- SCPs filter the permissions available to accounts
- Access is explicitly allowed or denied
- After access is specifically allowed; all other access is implicitly blocked
- The default AWS Organizations policy is full access

Creating an AWS Organization



Note; RAM - Resource Access Manager features