Best Practices for AWS Organizations Service Control Policies

Service Control Policies (SCPs) in AWS Organizations are a crucial part of implementing governance and compliance across an AWS environment. Here's the guidance on best practices for AWS Organizations Service Control Policies:

1. Understand Your Organization's Structure

- Clearly define your organizational units (OUs) based on business units, departments, or other logical groupings.
- Align SCPs with your organizational structure to ensure that policies are applied where they are most relevant.

2. Use SCPs to Enforce Security and Compliance

- Leverage SCPs to enforce security and compliance policies across your entire organization.
- Implement policies that restrict actions to only those necessary for business operations, minimizing unnecessary privileges.

3. Start with Least Privilege

- Begin with a default deny approach, allowing only the actions that are absolutely required for the organization's operations.
- Grant permissions on a need-to-have basis, minimizing the risk of unintended access.

4. Regularly Review and Update SCPs

- Periodically review and update your SCPs to adapt to changes in your organization's structure, policies, or regulatory requirements.
- Ensure that SCPs align with the latest AWS best practices and service offerings.

5. Test SCPs in a Staging Environment

- Before deploying SCPs in a production environment, test them in a staging environment to verify their impact on different accounts and services.
- Use AWS Organizations and AWS Identity and Access Management (IAM) simulated policy evaluations to assess the impact of SCP changes.

6. Implement Guardrails for Key Resources

- Identify critical resources and services, and implement SCPs as guardrails to prevent unintended actions on these resources.
- For example, use SCPs to restrict the deletion of critical Amazon S3 buckets or EC2 instances.

7. Document and Communicate SCP Policies

- Clearly document the purpose and impact of each SCP, and communicate these policies to relevant stakeholders.
- Ensure that there is a process in place for users to request exceptions or changes to SCPs when necessary.

8. Monitor and Audit SCP Compliance

- Implement monitoring and logging for SCP enforcement using AWS CloudTrail and AWS Config.
- Regularly audit SCP compliance to identify and remediate any deviations from the established policies.

9. Collaborate with Security and Compliance Teams

- Foster collaboration between the IT, security, and compliance teams to ensure that SCPs align with overall organizational security and compliance objectives.
- Use AWS Organizations to delegate management of specific OUs to different teams while maintaining overall governance.

10. Stay Informed About AWS Updates

- Stay informed about updates to AWS services and features that may impact SCPs.
- Leverage AWS resources, such as AWS blogs, documentation, and webinars, to stay current with best practices.

Remember, the key to effective SCPs is continuous evaluation, collaboration, and adaptation to the evolving needs and structure of your organization.

AWS Documentation