International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Customized Tagging of resources in AWS Account

Monalisa kaur

Customized tagging solution offers solution to apply user-provided tags to resources. Tags help organize

resources so that they can be easily filtered, tracked, and managed.

Tagged resources can be extremely helpful in improving billing and utilization monitoring by offering a flexible and granular way to categorize, track, and allocate resources within your cloud environment.

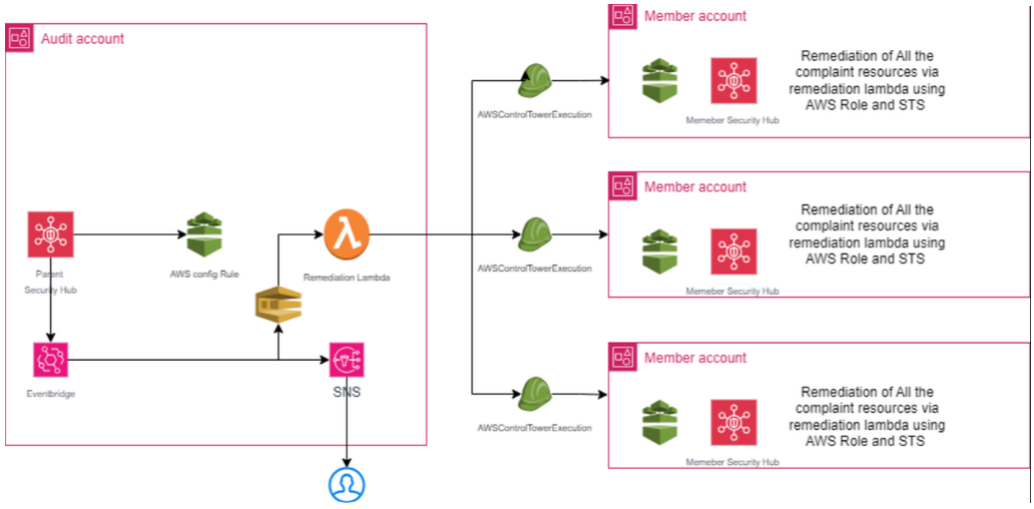
Tags can help track resource usage and costs associated with specific departments, teams, or projects (based on required tags) aiding in better cost allocation and budgeting.

This solution focuses on monitoring compliance of resources and remediation which involves converting non-compliant resources to compliant.

Prerequisites

Security hub should be enabled in audit account and all member accounts should be invited.

Quick Setup overview



1. Security hub helps to identify security issues, vulnerabilities, and misconfigurations in your AWS environment and provides actionable insights for remediation.
2. Deployment of code will create cloudformation stack in audit account which creates config rule named ‘required-tags-rule’, remediation lambda, eventbridge rule and SNS topic.
3. This solution can be deployed in multiple member accounts.
4. AWS Config rules evaluate the configuration settings of AWS resources. A rule can run when AWS Config detects a configuration change to an AWS resource or at a periodic frequency that you choose (for example, every 24 hours). In customized tagging solution, ‘required-tags-rule’ is created, it checks for resources in that account have required tags or not.
5. If AWS Config finds that resources don't have required tags, it generates a compliance finding that Security Hub can display as part of the security alerts, making it easy to spot and address.
6. EventBridge can listen to security findings from Security Hub and trigger remediation lambda for automated actions. Eventbridge will send notifications to user regarding security hub findings.
7. EventBridge puts the findings (as messages) into SQS. SQS queue holds the messages. Lambda reads the messages from SQS and performs remediation.

8. If the Lambda fails for some reason ,SQS can hold the message and allow the Lambda to retry processing it. This provides built-in **dead-letter queues (DLQs)** and **visibility timeout** mechanisms that can prevent data loss and help in error handling.
9. Remediation lambda adds tags to non-compliant resources.
10. **Multi-account deployment** -

Remediation lambda assumes 'AWSControlTowerExecution' role which is present in all accounts (including newly vended) by default. That role enables remediation lambda to remediate resources from other member accounts.

Use Case:

1. Improved Billing Tracking

- **Cost Allocation**: Tags allow you to assign specific metadata to your resources, such as projects, departments, or environments (e.g., "Marketing", "Production", or "Test"). This enables you to track and separate costs associated with different parts of your business.
  - **Example**: If you run different marketing campaigns, you can tag resources related to those campaigns (e.g., EC2 instances, databases, or storage) and easily calculate the costs related to each campaign.
- **Granular Billing Reports**: Many cloud platforms (e.g., AWS, Azure, GCP) allow you to generate detailed billing reports based on tags. You can view resource usage costs by tag, so you can break down expenses by department, project, or any other criteria that matter to your organization.
- **Accurate Chargeback/Showback**: In an organization with multiple departments or teams, tagged resources enable more accurate chargeback (allocating the cost to the respective department) or showback (informing teams of their usage and costs) models.

2. Simplified Reporting

- **Customized Dashboards and Metrics**: Many cloud management tools and monitoring platforms allow you to create custom dashboards based on tags. For example, you can have separate views for different departments or projects, allowing for better transparency in both billing and usage.
- **Trend Analysis**: By tracking resource usage and costs over time for specific tags, you can perform trend analysis. For example, you might notice that usage is increasing for resources tagged "Marketing", prompting you to allocate more resources or adjust budgets.

3. Policy and Governance

- **Compliance and Auditing**: With tags, you can track which resources are associated with specific departments, projects, or regulatory requirements. This makes auditing simpler and ensures compliance with internal policies.
- **Automation**: Some organizations automate the scaling or shutting down of resources based on tags. For instance, non-production resources tagged as "Test" might be scheduled to be turned off during off-hours to save costs.

4. Selective Resource Deletion

- **Tagging for Identification**: Tags are metadata that can be added to AWS resources. For example, you can use a tag such as `Environment=Test` or `Project=OldProject`. These tags help to classify resources based on specific criteria, such as the environment (e.g., production, staging, or development), project name, or owner.
- **Filter Resources**: Nuke scripts can be configured to only delete resources that have certain tags. For example, you might want to delete resources associated with a project that is no longer needed (i.e., `Project=OldProject`), but leave all resources tagged as `Environment=Production` untouched.
  - **Example Script**: A script could be written to delete only resources tagged with `Environment=Test` and `Project=OldProject`, preventing the deletion of critical resources like production instances.

5. Tagging to Safeguard Critical Resources

Excluding Critical Resources: One of the dangers of using nuke scripts is the possibility of accidentally deleting resources that are essential to your business operations, such as production databases or storage buckets. By adding specific tags to important resources, you can configure the nuke script to exclude these resources from deletion.

- **Example**: You could tag all production resources with `Critical=True`, and write the nuke script to skip any resource with this tag. This ensures that resources crucial to the business remain safe while cleaning up unused or outdated ones.

6. **Automated Cleanup by Lifecycle or Project Phase**

- **Time-Based Cleanup**: Tags can also be used to mark resources that are past their useful life. For instance, you can tag resources with `LifeCycle=Expired` or `Status=ToBeDeleted`. Nuke scripts can then target and delete only resources that are marked as expired or ready for cleanup.
  - **Example**: Resources tagged with `LifeCycle=Expired` could be cleaned up on a periodic basis, allowing for an automated and scheduled cleanup process that removes older, inactive resources without disrupting ongoing operations.

7. **Granular Control for Different Resource Types**

- **Resource-Specific Cleanup**: AWS resources such as EC2 instances, S3 buckets, or RDS databases can each have their own set of tags, making it possible to selectively clean up specific types of resources without impacting others.
  - **Example**: You can set up different tags for various AWS resource types, like `Service=EC2` for instances, `Service=S3` for storage buckets, and `Service=RDS` for databases. Nuke scripts can be configured to clean up only certain resource types (e.g., deleting only EC2 instances but leaving RDS databases intact).

8. **Auditing and Logging Cleanup Actions**

- **Track Deletion Events**: By tagging resources before cleanup, you create an easily auditable system. If you delete a resource as part of a cleanup process, you can trace back to the tag and identify why and when it was tagged for deletion.
- **Logging**: Nuke scripts can also generate logs that record which resources were deleted and why they were targeted for removal. This is useful for compliance or tracking the effectiveness of your cleanup operations.

Conclusion

In this post, we showed you how to setup customized tagging solution to tag aws resources.