大村 幸敬
アマゾン ウェブ サービス ジャパンソリューションアーキテクト
2020/2/17作成

AWS INNOVATE 2020 オンラインカンファレンス

「増加するシステムをマルチアカウントで効率よく管理する」の

クイズおよび解答

AWS INNOVATE 2020のセッションの視聴およびアンケートにご記入頂きありがとうございます。本資料が「増加するシステムをマルチアカウントで効率よく管理する」で出題されたクイズの解答になります。

問題１：特定のタグの付与を強制するにはどのような方法がありますか

解答例1:

2019年11月にリリースされた AWS Organizations のタグポリシーを使うのが効果的です。タグポリシーにより、特定のタグキーが存在すること、そのタグキーに設定できる値を指定すること、そのタグを強制するリソース、を指定することができます。このタグポリシーをOU(Organization Units)や特定のアカウントにアタッチすることで、このルールを強制することができます。詳しくはブログ「新機能 – タグポリシーを使用して、複数の AWS アカウントのタグを管理する」を参照してください。

Organizationsを使わず設定する方法としては、IAM Policy を使う方法があります。IAM Policy の設定によりEC2の作成などのAPIを呼び出す際に特定のタグが指定されていることを強制することができます。このIAM Policyを特定のIAMユーザーやIAM Roleに設定することでタグの使用を強制することができます。設定の例として、「新機能 – 作成時に EC2 インスタンスと EBS ボリュームにタグ付け」を参照してください。また、タグを使ったIAM制御が可能なリソースの一覧は「IAM と連携する AWS のサービス」に記載されています。

設定時に強制するのではなく、タグが付与されていないことを後から検出する方法もあります。AWS Config Rules の マネージドルールには「required-tags」というルールがあり、設定変更時に指定したタグが設定されているかどうかをチェックします。すべてのリソースをサポートしてはいないため、詳しくは「 AWS Config Rulesのドキュメント(required-tags)」をご覧ください。

大村 幸敬
アマゾン ウェブ サービス ジャパンソリューションアーキテクト
2020/2/17作成

参考資料

- 新機能 – タグポリシーを使用して、複数の AWS アカウントのタグを管理する
  https://aws.amazon.com/jp/blogs/news/new-use-tag-policies-to-manage-tags-across-multiple-aws-accounts/
- 新機能 – 作成時に EC2 インスタンスと EBS ボリュームにタグ付け
  https://aws.amazon.com/jp/blogs/news/new-tag-ec2-instances-ebs-volumes-on-creation/
- IAM と連携する AWS のサービス
  https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html
- AWS Config Rules のドキュメント（required-tags）
  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/required-tags.html

大村 幸敬
アマゾン ウェブ サービス ジャパンソリューションアーキテクト
2020/2/17作成

問題２：集約したログを定期的に監査するにはどのような方法がありますか

解答例2:

概して監査対象となるログは大量であり、また分析的な処理が必要となります。AWSの各種分析サービスを使うことで少ない実装で目的の監査結果を得ることができます。ログがS3に保存されているのであれば、Athenaを使ってクエリを実行し、条件に一致する結果を取得するといった方法が考えられます。ログがCloudWatch Logsに保存されているのであれば、CloudWatch Logs Insightsを使ってクエリを実行し、特定の属性を持つログを抽出したり、その頻度をグラフ化したりすることが可能です。これらの処理は CloudWatch Eventsを使ってLambdaファンクションを実行することで、定期的に呼び出したり、結果を通知したりすることが可能になります。AWS Summit Tokyo では「AWS で実現する攻めのシステムモニタリング」というタイトルでモニタリングから分析に至る流れを解説したセッションがありますので、こちらもご参照ください。

なお、AWSのAPI操作を記録するCloudTrailには通常と異なるアクティビティを自動的に検出・記録する CloudTrail Insights という機能があります（2019年11月リリース）。こちらも各アカウントにおける異常な操作を検出するために効果的です。

参考資料

- AWS で実現する攻めのシステムモニタリング
  https://www.youtube.com/watch?v=9MNMGqnYo68

大村 幸敬
アマゾン ウェブ サービス ジャパンソリューションアーキテクト
2020/2/17作成

問題3：発見的ガードレールで検知された事象を自動的に対応するにはどのような方法がありますか

解答3:

発見的ガードレールを実装する AWS Config Rules には修復アクションという機能があります。これによって、あるリソースが Config Rules で指定されたルールを逸脱した（非準拠になった）際に、修復のため Systems Manager の Automation を自動的にキックすることができ、これによってリソースを準拠状態に回復させたり、通知を行ったりすることが可能です。Config Rulesでは検知だけを行い、Automation を手動でキックすることも可能です。詳しくは「AWS Config Rules による 非準拠 AWS リソースの修復」をご参照ください。なお、修復アクションを使う方法の他に、CloudWatch Events でステータス変更を通知し、Lambdaで対処を行うことも可能です。この場合はルールからの逸脱だけでなく、構成変更のすべてのイベントをトリガにして処理を記述するといったこともできます。

Systems Manager の Automation は 任意のAWS APIを使って処理を記述することができるため、多様な処理が可能です。AWSが標準で提供しているAutomation ドキュメント（手順）には、EC2インスタンスの再起動や、SNSメッセージの発行（この先でLambdaを実行することが可能）など、よく実行される手順が用意されています。このほか、独自にAutomation ドキュメントを作成してご自身の環境にあった処理手順を作成することができます。2019年11月に 「Automation ドキュメント ビルダー」という機能がリリースされ、直接PythonやPowerShellのコードを書くこともできるようになり、独自ドキュメントがより作成しやすくなりました。詳しくは「AWS Systems Manager の新しいオートメーション機能」をご参照ください。

参考資料

- AWS Config Rules による 非準拠 AWS リソースの修復
  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/remediation.html

大村 幸敬
アマゾン ウェブ サービス ジャパンソリューションアーキテクト
2020/2/17作成

- Amazon CloudWatch Events を使用した AWS Config のモニタリング
  https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/monitor-config-with-cloudwatchevents.html
- AWS Systems Manager の新しいオートメーション機能
  https://aws.amazon.com/jp/blogs/news/new-automation-features-in-aws-systems-manager/

マルチアカウント管理についてのその他の参考資料

- クラウド運用管理の最前線 ～日米の最新状況から～
  https://pages.awscloud.com/rs/112-TZM-766/images/A1-06.pdf
- マルチアカウント運用での権限移譲と統制の両立
  https://pages.awscloud.com/rs/112-TZM-766/images/B2-07.pdf
- AWS Black Belt Online Seminar AWS のマネジメント&ガバナンス サービスアップデート
  https://www.slideshare.net/AmazonWebServicesJapan/20191218-aws-black-belt-online-seminar-aws