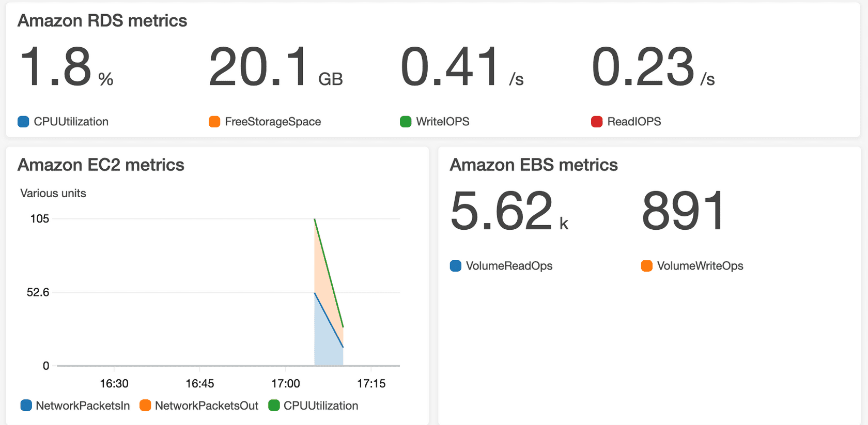
1. Amazon CloudWatch

様々な指標をモニタリング及び管理し、当該指標のデータに基づいて警報作業を構成できるウェブサービス  
 AWSサービスは、指標をCloudWatchに送る。 すると、CloudWatchがこのような指標を使用して、時間の経過とともに性能がどのように変化したかを示すグラフを自動的に生成  
  
 1) CloudWatchアラート  
 CloudWatchを使用すると、指標の値があらかじめ定義されたしきい値を上回ったり下回ったりする場合、自動的に作業を行うアラートを生成  
 例）アプリケーション開発またはテストのためにAmazon EC2 インスタンスを使用する -> たまにインスタンスを停止するのを忘れた場合、インスタンスが実行され続けて料金が発生する  
 => CPU使用率が指定された期間中、特定のしきい値未満に維持されると、Amazon EC2 インスタンスを自動的に中止するCloudWatch アラートを生成することができる。  
  
 2) CloudWatchダッシュボード



Amazon EC2 インスタンスのCPU 使用率、Amazon S3 バケットに対して実行された総要請数などをモニタリングできる。

2. AWS CloudTrail

アカウントへのAPI呼び出しを記録  
 誰かが残した移動経路（またはジョブログ）の「追跡」  
 記録される情報にはAPI呼出者ID、API呼出時間、API呼出者のソースIPアドレスなどが含まれる  
  
 例) AWS CloudTrailイベント  
 新しいIAMユーザーが生成されたことは発見したが、このユーザーを作った人、時期、または方法は分からない->解決するためにAWS CloudTrailに移動する。  
  
 何が起こりましたか？ : 新しいIAMユーザー(Mary)が作成された  
 誰が要請しましたか？ : IAMユーザーJohn  
 いつ発生しましたか？ : 2020年1月1日の午前9:00  
 どのように要請しましたか？ : AWS管理コンソールにより  
  
 CloudTrailイベント記録セクションでIAMの「CreateUser」API作業に対するイベントだけを表示するようにフィルターを適用->その結果、MaryというIAMユーザーを生成したAPI呼び出しに対するイベントを探す->このイベントレコードは発生した作業に対する全体の詳細情報を提供します

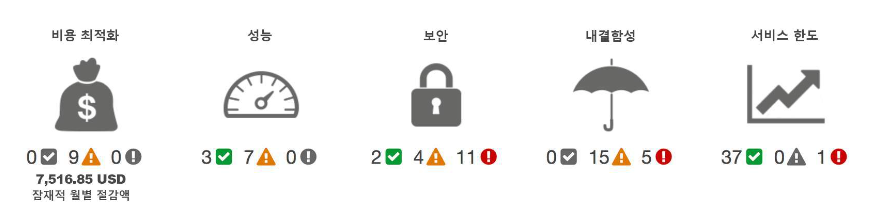
1) CloudTrail Insights

CloudTrailでCloudTrail Insightsを有効にすることもできる。  
 このオプション機能を使用すると、CloudTrailがAWSアカウントで異常なAPI活動を自動的に検出することができる。

3. AWS Trusted Advisor

AWS環境を検査し、AWSのベストプラクティスに従ってリアルタイムで推奨事項を提示するウェブサービス  
 オープンアクセス権限を確認し、Amazon S3バケットのセキュリティを検討できるサービス

1) AWS Trusted Advisorダッシュボード



AWS管理コンソールでTrusted Advisorダッシュボードにアクセスすると、コスト最適化、性能、セキュリティ、耐欠陥性、サービス限度のカテゴリで完了した検査を検討することができる。  
  
 - 緑色チェック表示は問題が感知されていない項目数を示す。  
 - オレンジ色の三角形は推奨調査項目数を示す。  
 - 赤色の円は推奨処置数を示す。