Alibaba Cloud
操作##

ベストプラクティス

Document Version20200313

目次

1 ActionTrail を通じて AccessKey の使用をモニタリングする

本ドキュメントでは、**ActionTrail** を通じて **AccessKey** の使用をモニタリングする方法について説明します。 履歴イベントのチェックや、トレイルを設定してトレイルイベントを **Log Service** へ送信することによって **AccessKey** のモニタリングなどで、過去 **30** 日間の **AccessKey** の使用状況を確認できます。

履歴イベントのクエリ

ActionTrail サービスを有効にすることで、過去 **30** 日間に発生したトレイルイベントを表示できます。

1. *ActionTrail コンソール*にログインします。
2. 左側のメニューで、履歴検索をクリックします。
3. フィルタードロップダウンリストから、**AccessKeyId** を選択します。
4. **AccessKeyId** を入力してトレイルイベントを検索します。

> 注：
> 左上隅のリージョンを切り替えることで、さまざまなリージョンの **AccessKeyId** によって使用されるトレイルイベントを表示できます。

トレイルの使用

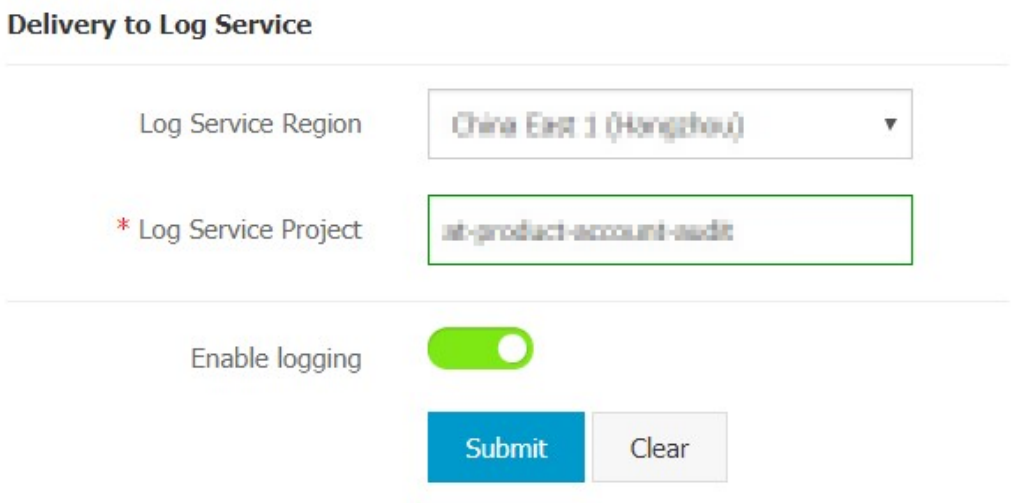
ActionTrail では、トレイルイベントを **Log Service** に送信することで **AccessKey** をモニタリングできます。

1. 左側のメニューで、トレイルリストをクリックします。
2. トレイルの作成をクリックします。
3. 監査イベントを **LogService** に送信を選択した場合、**Log Service** リージョンと**Log Service** プロジェクトを設定する必要があります。

> 注：
> プロジェクトは **ActionTrail** ログを保存するために使用されます。 選択したリージョンの下にプロジェクト名を入力するか、新しいプロジェクト名を入力できます。

4. ログを有効にするを選択します。

5. 送信をクリックします。



トレイルを作成後、**ActionTrail** はすべてのリージョンのトレイルイベントを自動的に指定された **Logstore** に送信します。

Log Service の設定

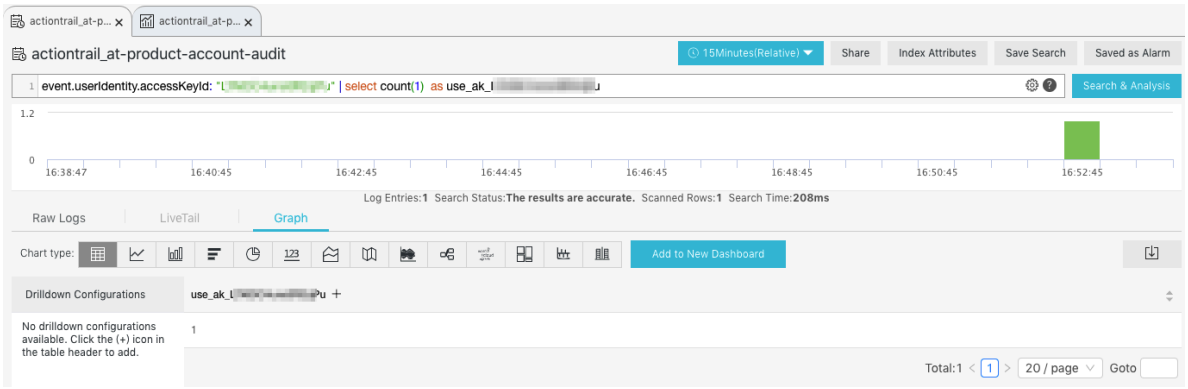
Log Service には、データ分析、レポート作成、およびアラームを含む複数の機能があります。アラームの設定方法は次の通りです。

1. *Log Service コンソール*にログインします。
2. プロジェクトをクリックします。
3. **Logstore** リストページで、対象の **Logstore** の検索をクリックします。
4. 必要に応じて **Logstore**、**Topic**、クエリ **SQL** ステートメントを指定して、ログを検索します。

> 注：
> ページの右上隅にあるクイック検索として保存をクリックして、クイック検索用のパラメータを保存できます。

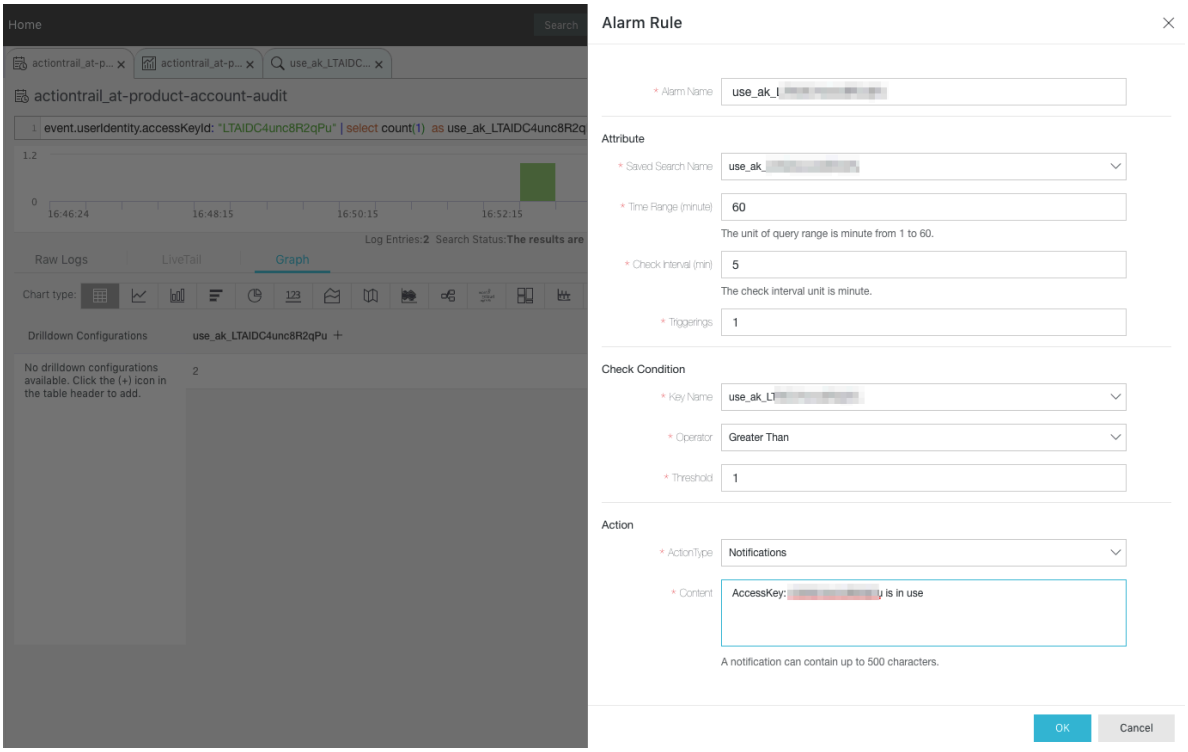
クエリ SQL ステートメントの例：

```
event.userIdentity.accessKeyId: "LTAIDC4unc8R2qPu" | select count(1) as use_ak_LTAIDC4unc8R2qPu
```



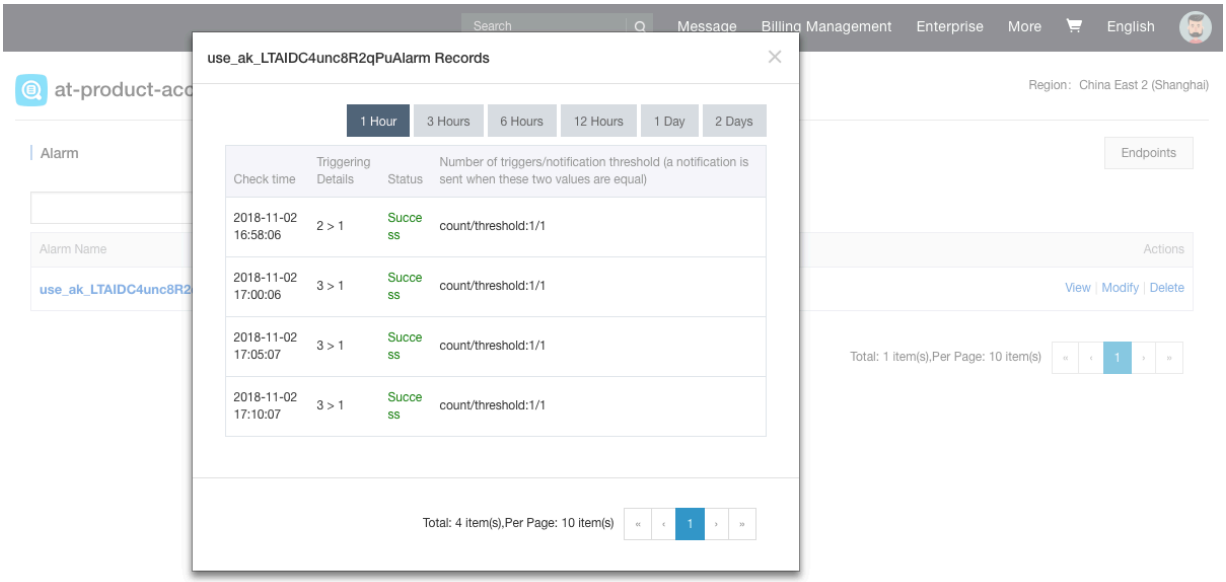
5. 保存したクイック検索に基づいてアラームを作成し、ページの右上隅にあるアラームとして保存をクリックします。

> 注：
> チェック間隔を 5 に設定した場合、過去 10 分間のデータが 5 分間隔でチェックされます。accessKeyId（LTAIDC4unc8R2qPuなど）が 10 分に 1 回使用されると、アラームが生成されます。

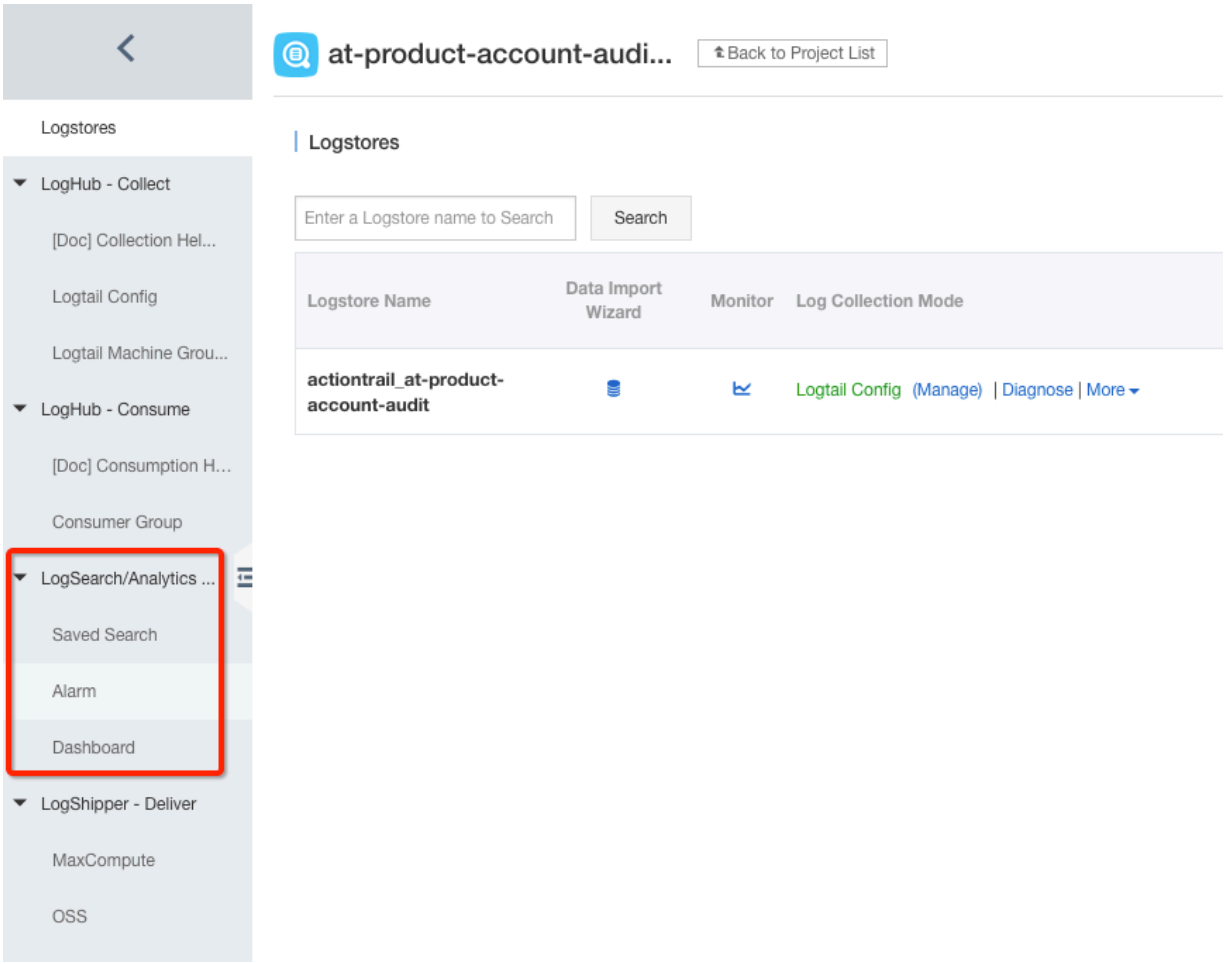


アラームの例は次の通りです：

『*[Alibaba Cloud] Log Service alarm: The project henshao-test-send-sls-600/trigger use_ak_b7z of 71887**@qq.com takes effect 2 > 1; content: AccessKey: LTAIDC4unc8R2qPu is in use. Context: [use_ak_LTAIDC4unc8R2qPu:2]*』



プロジェクトページで、保存したクイック検索及びアラームを表示および管理できます。



Log Service は、通知、**SMS**、**WebHook-DingTalk Bot**、**WebHook-Custom** など、さまざまな種類のアラームをサポートしています。 必要に応じて適切な種類を選択できます。

2 ActionTrail 操作と RAM でサポートされているリソース

Alibaba Cloud RAM を使用して **RAM** アカウントを作成し、**RAM** アカウントに **ActionTrail** を操作する権限を付与することができます。 セキュリティの観点から、このアプローチを強くお勧めします。

RAM アカウントに権限付与できる ActionTrail 操作のリスト

RAM アカウントに権限付与できる **ActionTrail** 操作は次のとおりです。

- **CreateTrail**
- **UpdateTrail**
- **DeleteTrail**
- **DescribeTrails**
- **GetTrailStatus**
- **StartLogging**
- **StopLogging**
- **LookupEvents**

リソースのフォーマット

Alibaba Cloud のリソースは、**RAM** アカウントへのアクセス権限を付与するときに次のようにフォーマットされます。

リソース	説明
*	すべてのクラウドリソース。
acs:actiontrail:${region}:${AccountId}:*	特定のリージョンのリソース。

権限付与ポリシーの例

- 読み取り専用操作を許可する

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*"
```

```
    }]
}
```

・ 特定の IP 範囲からの読み取り専用操作を許可する

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*",
        "Condition":{
            "IpAddress": {
                "acs:SourceIp": "42.120.66.0/24"
            }
        }
    }]
}
```

3 RAM ユーザーへの ActionTrail 権限の付与

前提条件

#unique_4 .

ActionTrail システム権限付与ポリシーをグループに割り当て

使用可能なシステム権限付与ポリシーは次のとおりです。

- **AliyunActionTrailReadOnlyAccess**（読み取り専用アクセス権限）
- **AliyunActionTrailFullAccess**（フルアクセス権限）

ポリシーを割り当てる方法については、*#unique_5*をご参照ください。

カスタマイズされた権限付与ポリシーをグループに割り当て

システム権限付与ポリシーが要件を満たさない場合は、*#unique_6*をすることができます。 下記は、特定の **IP** 範囲からの、すべてのリソースに対する **ActionTrail** 読み取り専用操作のリクエストを許可するポリシーの例です。

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*",
        "Condition":{
            "IpAddress": {
                "acs:SourceIp": "42.120.66.0/24"
            }
        }
    }]
}
```