# Nordcloud Klarity CloudTrail Activity Events

* [Nordcloud Klarity CloudTrail Activity Events](#Xd803ed10738175648f9596f6b34b05f71dea562)
  + [AWS CloudTrail Activity Events](#aws-cloudtrail-activity-events)
    - [AWS CloudTrail partner](#aws-cloudtrail-partner)
    - [Event Schema](#event-schema)
    - [Getting started](#getting-started)
  + [Nordcloud Klarity](#nordcloud-klarity)
    - [AWS CloudTrail integration](#aws-cloudtrail-integration)
    - [Enabling integration in AWS Console](#enabling-integration-in-aws-console)
    - [Disabling integration](#disabling-integration)
    - [Event Sources](#event-sources)
    - [Event Types](#event-types)
  + [Architecture](#architecture)
  + [Examples](#examples)
  + [Support](#support)

## AWS CloudTrail Activity Events

AWS CloudTrail Lake let you use CloudTrail to log and store user activity data from any source in your hybrid environments, such as in-house or SaaS applications hosted on-premises or in the cloud, virtual machines, or containers. You can store, access, analyze, troubleshoot and take action on this data without maintaining multiple log aggregators and reporting tools.

Once you get event data from third-party application or via PutAuditEvents API, you can create event data stores in AWS CloudTrail Lake, and use it to search, query, and analyze the data that is logged from your applications. To help you meet compliance resources this data is backed by a 7-year default retention period.

For more information, please refer to official [AWS documentation](https://docs.aws.amazon.com/).

### AWS CloudTrail partner

AWS CloudTrail Lake supports ingesting activity logs from the trusted entities like Nordcloud Klarity that is being an official AWS Partner in CloudTrail Lake activity events.

AWS and Klarity teams works together to deliver this integration allowing you to simplify the process of consolidating activity data. It enables the enhanced visibility across applications and environments. In a few steps you can consolidate Klarity activity logs together with AWS activity logs without having additional processing pipelines.

To get started with Klarity integration please refer to go to the [AWS CloudTrail integration](#aws-cloudtrail-integration) section.

### Event Schema

The following example shows the complete schema of event records that can be ingested to AWS CloudTrail Lake. The content of eventData is provided by the application that is publishing the event. Other fields are provided by AWS CloudTrail.

{  
 "eventID": "string",  
 "eventVersion": "string",  
 "eventCategory": "string",  
 "eventType": "string",  
 "eventTime": "string",  
 "awsRegion": "string",  
 "recipientAccountId": "string",  
 "addendum": {  
 "reason": "string",  
 "updatedFields": "string",  
 "originalUID": "string",  
 "originalEventID": "string"  
 },  
 "metadata" : {  
 "ingestionTime": "string",  
 "channelARN": "string"  
 },  
 "eventData": {  
 "version": "string",  
 "userIdentity": {  
 "type": "string",  
 "principalId": "string",  
 "details": { JSON }  
 },  
 "userAgent": "string",  
 "eventSource": "string",  
 "eventName": "string",  
 "eventTime": "string",  
 "UID": "string",  
 "requestParameters": { JSON },  
 "responseElements": { JSON },  
 "errorCode": "string",  
 "errorMessage": "string",  
 "sourceIPAddress": "string",  
 "recipientAccountId": "string",  
 "additionalEventData": { JSON }  
 }  
}

For more information, please refer to official [AWS documentation](https://docs.aws.amazon.com/).

### Getting started

To receive CloudTrail Events from third-party applications like Nordcloud Klarity following actions are required:

1. Create an IAM role that allows third-party applications to use AWS CloudTrail API. IAM policy can be found in [policy.json](https://github.com/nordcloud/klarity-cloudtrail-activity-events/tree/main/policy.json) file.
2. Create Event Data Store in AWS CloudTrail Lake to store incoming events. You can do that by running the following API call:

* aws cloudtrail create-event-data-store \  
   --name my-event-data-store \  
   --retention-period 90

1. Create an ingestion channel to ingest events from a third-party application. You can do that by running the following API call:

* aws cloudtrail create-channel \  
   --region us-east-1 \  
   --name my-customer-ingestion-channel \  
   --source-name $partnerSourceName \  
   --destinations '[{"Type": "EventDataStore", "Location": "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}]'

1. Use the PutAuditEvents API to load events from your third-party application:

* aws cloudtrail-data put-audit-events \  
   --channel-arn $ChannelArn \  
   --audit-events \  
   {  
   "AuditEvents": [  
   {  
   "Id": "original\_event\_ID",  
   "EventData": "{event\_payload}",  
   }  
   ]  
   }

For more details, please refer to official [AWS documentation](https://docs.aws.amazon.com/).

## Nordcloud Klarity

Nordcloud Klarity was developed by Nordcloud, an IBM Company, the European leader in cloud migration, application development and managed services. We like to say Nordcloud Klarity is like autopilot for cloud management, because our goal is to help businesses manage cloud costs, automate operations, improve security and accelerate development with no manual work.

Currently, there are four Nordcloud Klarity tools in the toolkit:

* [Nordcloud Klarity Core](https://klarity.nordcloud.com/products/klarity-core/)
* [Nordcloud Klarity ImageFactory](https://klarity.nordcloud.com/products/klarity-imagefactory/)
* [Nordcloud Klarity AutoPatcher](https://klarity.nordcloud.com/products/klarity-autopatcher/)
* [Nordcloud Klarity AutoBackup](https://klarity.nordcloud.com/products/klarity-autopatcher/)

Together, this suite of cloud management tools gives you the facts you need to understand and optimize your cloud costs, infrastructure, security and data, empowering you to make strategic business decisions.

### AWS CloudTrail integration

Nordcloud Klarity is integrated with Cloud Trail Lake to store and monitor customer tenant activity. You can enable this integration to receive logs on activities in your application tenant. Events published by the Nordcloud Klarity can be related to the actions performed by applications on customer cloud environments or any other tenant activity.

Ingested events are stored in the customer AWS account in Cloud Trail Lake Data Store. Customers can run queries or any other processing on this data.

Example use cases for using Cloud Trail Events:

* Monitor user activity on application tenant.
* Store and analyze tenant configuration changes.
* Monitor actions executed by the SaaS application on customer AWS accounts or any other environment used by the application.
* Ensure company compliance by directly accessing all events produced by a third-party application.

***Nordcloud Klarity is an AWS partner in AWS CloudTrail Lake integration. It makes it a trusted source of events and simplifies the integration process.***

### Enabling integration in AWS Console

Nordcloud Klarity is AWS Partner in AWS CloudTrail Lake so it should be possible to easily enable this integration in AWS Console.

Please navigate to AWS CloudTrail console where you have a CloudTrail Lake event data store enabled. You will be guided on how to enable integration by selecting Nordcloud Klarity from the list of AWS CloudTrail partners.

Next step is to Provide Nordcloud Klarity with IAM role permissions to call PutAuditEvents API on your behalf. IAM permissions define actions that a principal can perform (or is restricted from performing). The permissions define resources on which the actions can (or cannot) be taken.

{  
 "Effect": "Allow",  
 "Action": "cloudtrail-data:PutAuditEvents",  
 "Resource": "<Channel ARN>"  
}

A trust policy defines which principals can assume the role, and under which conditions. This is sometimes called a resource-based policy for the role.

{  
 "Effect": "Allow",  
 "Principal": {  
 "AWS": "arn:aws:iam::855341727128:root"  
 },  
 "Action": "sts:AssumeRole",  
 "Condition": {  
 "StringEquals": {  
 "sts:ExternalId": "<Channel ARN>"  
 }  
 }  
}

For more information, please refer to official [AWS documentation](https://aws.amazon.com/blogs/aws/new-aws-cloudtrail-lake-supports-ingesting-activity-events-from-non-aws-sources/).

Once you have created IAM role and CloudTrail ingestion channel please contact with your CSM and provide following information:

* IAM role arn
* Ingestion channel ARN

Please note that at the beginning not all Klarity tools will implement AWS CloudTrail activity events. This will be delivered based on our roadmap and customer requirements. To ask for feature availability please contact with your CSM.

### Disabling integration

To disable integration simply navigate to the AWS CloudTrail console and disable integration with Nordcloud Klarity. If you want to remove it completely please remove the created IAM role as well.

### Event Sources

A single and unique event source is reserved for each of Klarity tool. Currently, we we have secured the following event sources:

| Klarity tool name | Event Source | Integration enabled |
| --- | --- | --- |
| Nordcloud Klarity Core | com.nordcloudapp.com.klarity | ❌ |
| Nordcloud Klarity ImageFactory | com.nordcloudapp.com.imagefactory | ❌ |
| Nordcloud Klarity AutoBackup | com.nordcloudapp.com.autobackup | ❌ |
| Nordcloud Klarity AutoPatcher | com.nordcloudapp.com.autopatcher | ❌ |

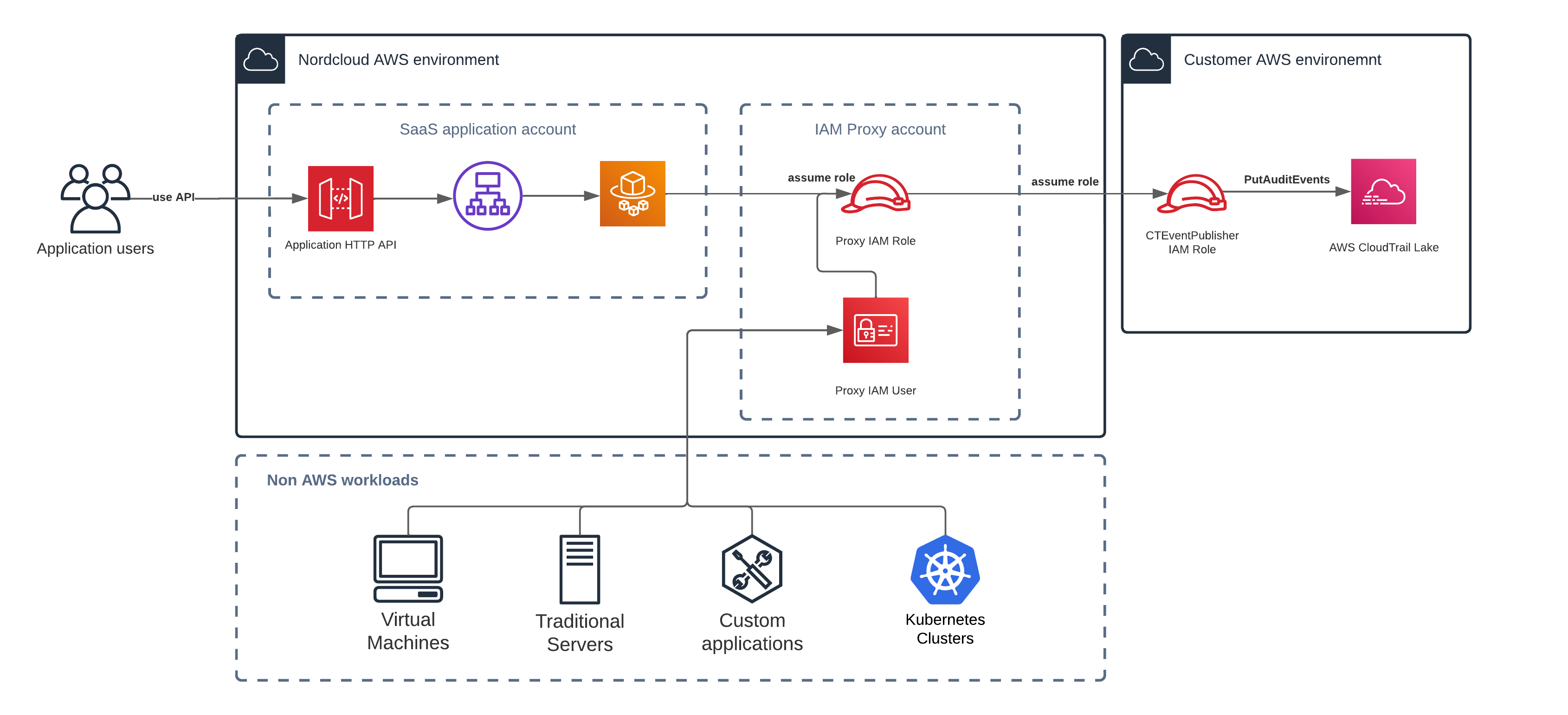
Please note that the above list may change in the future once we add new applications to the Klarity.

❌ - *The Event source name is reserved for the application but integration is not yet fully implemented.* ✅ - *Integration is fully implemented.*

### Event Types

Event types define the activity that happened on the application tenant or operation executed by the application in the cloud environment. Every Klarity tool has its own uniq set of events depending on the functionality. Please check the application specific documentation in the [event-sources](https://github.com/nordcloud/klarity-cloudtrail-activity-events/tree/main/event-sources) directory for more details.

## Architecture



Integration diagram

## Examples

As an example, the following activity event is produced by the Klarity Core as an result of creating new discovery rule in test env environment by name@example.com user.

{  
 "eventData": {  
 "version": "v1",  
 "userIdentity": {  
 "type": "USER",  
 "principalId": "name@example.com"  
 },  
 "eventSource": "com.nordcloudapp.com.klarity",  
 "eventName": "discoveryRule.created",  
 "eventTime": "2022-07-12T10:55:00",  
 "UID": "00000000-00000000-00000000-00000000",  
 "requestParameters": {  
 "ruleName": "rule name",  
 "ruleId": "00000000-00000000-00000000-00000001",  
 "environment": "test env",  
 "application": "test app"  
 }  
 }  
}

You can find a documentation on all activity events produced by the Klarity tools in the [event-sources](https://github.com/nordcloud/klarity-cloudtrail-activity-events/tree/main/event-sources) directory.

## Support

To get support on the Nordcloud Klarity CloudTrail integration please contact with your CSM or create ticket using Nordcloud Klarity Jira Service Desk.

We strongly encourage you to leave us a feedback regarding this functionality. New applications and events are going to be delivered based on customer demands.