# Table of Contents

Welcome ............................................................................................................................................. 1
Cost ...................................................................................................................................................... 2
Architecture overview .......................................................................................................................... 3
Solution components ............................................................................................................................ 4
  Web interface ...................................................................................................................................... 4
  Data Analysis ..................................................................................................................................... 4
  AWS AppSync ..................................................................................................................................... 5
External integrations .............................................................................................................................. 5
  Amazon Lookout for Equipment ....................................................................................................... 5
  IoT devices ........................................................................................................................................ 5
  Other Systems ................................................................................................................................... 5
  API ................................................................................................................................................... 6
Amazon Cognito user groups .................................................................................................................. 15
Amazon DynamoDB .............................................................................................................................. 17
AWS IoT Core ....................................................................................................................................... 17
Solution microservices .......................................................................................................................... 17
  AWS AppSync Lambda resolver microservice ................................................................................ 17
  Handle issues microservice ............................................................................................................. 17
  Amazon Cognito trigger microservice .............................................................................................. 17
  Solution helper microservice .......................................................................................................... 18
  External integrations microservice .................................................................................................. 18
Security .................................................................................................................................................. 19
  IAM Roles ........................................................................................................................................ 19
  Amazon CloudFront .......................................................................................................................... 19
  Amazon S3 Buckets ........................................................................................................................... 19
  Amazon Cognito ................................................................................................................................ 19
  SAML identity provider .................................................................................................................... 19
Considerations ......................................................................................................................................... 21
  Architecture with all optional resources ....................................................................................... 21
  Amazon Cognito limits ...................................................................................................................... 22
  Regional deployments ...................................................................................................................... 22
  Solution updates ............................................................................................................................... 22
AWS CloudFormation template ............................................................................................................. 23
Automated deployment ......................................................................................................................... 24
  Deployment overview ....................................................................................................................... 24
  Step 1. Launch the stack .................................................................................................................... 24
  Step 2. Sign in to the web interface ................................................................................................... 27
  Step 3. Add users .............................................................................................................................. 27
  Step 4. Add the root causes ............................................................................................................. 28
  Step 5. Add site details ..................................................................................................................... 28
  Optional: Configure Amazon Lookout for Equipment ....................................................................... 30
  Optional: Configure IoT devices ...................................................................................................... 30
  Step 6. Add permissions for users in the Associate Group .............................................................. 31
Additional resources ............................................................................................................................. 33
Solution web interface ........................................................................................................................... 34
  Management pages ........................................................................................................................... 34
    Sites page ......................................................................................................................................... 34
    Users page ........................................................................................................................................ 35
    Root causes page ............................................................................................................................ 36
    Permissions page ............................................................................................................................. 36
Client page ............................................................................................................................................... 36
Observer page .......................................................................................................................................... 37
Data analytics .......................................................................................................................................... 38
  Issues reporting ................................................................................................................................ 38
Set up a scalable Andon system and workflow to monitor manufacturing workstations and support the transition to predictive maintenance

Publication date: November 2019 (last update (p. 47): October 2021)

The Virtual Andon on AWS solution simplifies the process of monitoring manufacturing workstations, devices, and events. This solution provides a scalable, digital Andon system to help optimize processes, support the transition to predictive maintenance, and prevent future equipment issues. It also provides a workflow to help users monitor manufacturing workstations for an event, log the event, and then route the event to the correct engineer for resolution.

The Virtual Andon on AWS solution deploys a web interface to help administrators to define their factory setup, site name, process type, event types for each process, and lists of workstations.

This solution offers the following features:

- **Scalable Andon system:** Flexible integration to critical areas and work cells, or the entire facility.
- **Flexible management tools:** Observer view to manage open issues and the ability to run reporting on issue resolution.
- **Customizable web interface:** Configure events, root causes, and assignments to address issues immediately.
- **Multi-language support:** The web interface supports seven languages (German, English, Spanish, French, Japanese, Korean, and simplified Chinese) for factory settings, communications, and data analysis.

This implementation guide discusses architectural considerations and configuration steps for deploying Virtual Andon on AWS in the Amazon Web Services (AWS) Cloud. It includes links to an AWS CloudFormation template that launches and configures the AWS services required to deploy this solution using AWS best practices for security and availability.

The guide is intended for IT and operational infrastructure architects, administrators, and DevOps professionals who have practical experience with AWS IoT Core, and architecting in the AWS Cloud.
Cost

You are responsible for the cost of the AWS services used while running this solution. The total cost for running this solution depends on the amount of data being sent and processed. As of October 2021, the cost for running this solution with default settings in the US East (N. Virginia) Region is approximately $12.92 per month. The cost estimate assumes the following factors:

<table>
<thead>
<tr>
<th>AWS service</th>
<th>Dimensions</th>
<th>Cost per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Lambda</td>
<td>1M invocations of the HandleIssues function</td>
<td>$2.70</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>1 GB Data Storage, 1M write capacity units &amp; 1M read capacity units using On-Demand capacity mode</td>
<td>$1.75</td>
</tr>
<tr>
<td>AWS AppSync</td>
<td>1M query/data modification operations, 1M real-time updates, 1M minutes of connectivity</td>
<td>$6.17</td>
</tr>
<tr>
<td>AWS IoT Core</td>
<td>1M messages transmitted, 1M rules activated</td>
<td>$1.30</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>2 GB log data ingested</td>
<td>$1.00</td>
</tr>
</tbody>
</table>

**Total monthly cost:** $12.92

**Note**

If the Activate Glue Workflow parameter is set to Yes, there will be an additional AWS Glue cost of approximately $5.00 for the weekly data extract jobs. This estimate is based on approximately 2.5 Data Processing Units (DPU)-hours for the AWS Glue crawler and 7.5 hours for Glue jobs in the US East (N. Virginia) Region.

Prices are subject to change. This cost estimate does not reflect variable charges incurred from Amazon CloudFront and data transfers. For full details, refer to the pricing webpage for each AWS service used in this solution.
Architecture overview

Deploying this solution with the default parameters builds the following environment in the AWS Cloud.

The AWS CloudFormation template deploys the following infrastructure:

1. The AWS CloudFormation template provides an Amazon CloudFront web interface that deploys into an Amazon Simple Storage Service (Amazon S3) bucket configured for web hosting.
2. An Amazon Cognito user pool allows this solution's administrators to register users and groups using the web interface.
3. AWS AppSync GraphQL APIs and AWS Amplify power the web interface. Amazon DynamoDB tables store the factory data.
4. An AWS IoT rule engine helps users monitor manufacturing workstations or devices for events, and then routes the event to the correct engineer for resolution in real-time.
5. Authorized users can interact with and receive notifications from this solution. An AWS Lambda function and Amazon Simple Notification Service (Amazon SNS) send emails and SMS notifications.
6. Issues created, acknowledged, and closed in the web interface are recorded and updated using AWS AppSync and DynamoDB.
7. The AWS AppSync GraphQL APIs can be called directly (p. 5) with HTTP POST requests.

Figure 1: Virtual Andon on AWS architecture on AWS
Solution components

Web interface

The Virtual Andon on AWS solution features a web interface that simplifies managing factory settings, notifications, and data analysis. The interface leverages Amazon Cognito for user authentication, AWS Amplify for interacting with cloud services, and an Amazon Simple Storage Service (Amazon S3) bucket to host web assets.

Figure 2: Virtual Andon on AWS web interface

As shown in Figure 2, the web interface provides the following menu options: Sites, Client, Observer, Issues Reporting, Users, Permissions, and Root Causes. These options provide users with the following features:

- **Management tools**: These tools include the Sites, Users, Permissions, and Root Causes menu options. Administrators use these tools to manage users (such as factory floor workers, engineers, and managers), assign them to one or more specialized groups (refer to Amazon Cognito user groups (p. 15)), and enter the factory details for their facility. Administrators use the Sites option to define a factory using the following criteria: sites, areas, processes, stations, devices, and event details.

- **Analysis tools**: Users assigned to the Admin and Manager groups have access to the Issues Reporting tab. Users can view the historical information about issues that have occurred.

- **Client tool**: This tool is provided in the Client menu option. Users identify events or issues on the factory floor using this tool. If a point-of-contact (such as an engineer) is assigned to the event, an Amazon Simple Notification Service (Amazon SNS) notification is sent.

- **Observer function**: This function is provided in the Observer menu option. Users assigned to the Admin, Manager, and Engineer groups can access a real-time view of events across the factory site and respond to issues. Responses are recorded and synchronized in the web interface.

In order to access the web interface, the solution administrator must add users and assign them to one or more groups. Groups provide the users with the appropriate access privileges to the tools and functionalities available in the web interface. For details about setting up the web interface, refer to Automated deployment (p. 24). For more information about the web interface, refer to Solution web interface (p. 34).

The web interface supports the following languages: German, English, Spanish, French, Japanese, Korean, and simplified Chinese.

Data Analysis

Events and issues recorded and stored in this solution can be exported from DynamoDB to an Amazon S3 bucket for in-depth analysis and visualization in Amazon Athena, Amazon QuickSight, or your own BI tool. To do this, set the Activate Glue Workflow parameter to Yes when you deploy the CloudFormation template. For more information, refer to AWS Glue data export (p. 38).

By default, the AWS Glue workflow that performs the data extract runs every Monday at 1:00 AM UTC.
AWS AppSync

The solution uses AWS AppSync queries, mutations, and subscriptions generated by the AppSync schema. These queries, mutations, and subscriptions help set up the factory with management tools and real-time issue updates.

External integrations

Amazon Lookout for Equipment

This solution can integrate with Amazon Lookout for Equipment and automatically raise issues when anomalies are detected in machine telemetry data that Lookout for Equipment is monitoring. If Lookout for Equipment is delivering files to an Amazon S3 bucket containing anomaly data, you can supply the name of that bucket in the Anomaly Detection Output Bucket parameter. When anomaly files are placed in that bucket, an AWS Lambda function will be invoked to determine whether an anomaly is detected. If so, the function searches for both a matching automated Virtual Andon on AWS event and device. If found, an issue is created.

If integrating Lookout for Equipment, you can create an automated event in the solution’s web interface. Refer to Configure Amazon Lookout for Equipment (p. 30) for more information.

IoT devices

This solution uses AWS IoT Core, allowing you to configure your IoT devices to send data to the solution’s ava/devices IoT Core topic. To do this, the IoT device names must be created in the solution and contain the necessary Event tag and corresponding values. For guidance to set up your IoT devices, refer to Configure IoT devices (p. 30).

Other Systems

The Virtual Andon on AWS solution allows data to be easily integrated from other systems. To create issues in the solution originating from other devices, post a message to the ava/issues AWS IoT Core topic in the following format:

```
{
  "id": <ID!>,
  "eventId": String,
  "eventDescription": String,
  "type": String,
  "priority": String,
  "siteName": String,
  "processName": String,
  "areaName": String,
  "stationName": String,
  "deviceName": String,
  "created": AWSDateTime,
  "acknowledged": AWSDateTime,
  "closed": AWSDateTime,
  "status": "open"
}
```

Note

Set up the siteName, processName, areaName, stationName, deviceName, and eventDescription from the management UI before sending data to this topic. This ensures consistency across the observer UI and provides accurate information to engineers.
If you need support connecting to industrial equipment, refer to the Machine to Cloud Connectivity Framework solution. You can create an IoT rule to start an AWS Lambda function that can convert your machine data into the specified format and then publish the message to the ava/issues topic.

The format can also be used to call the `createIssue` AppSync mutation directly using an AWS AppSync client. For more information about building a NodeJS AppSync client, refer to Create a Client Application in the AWS AppSync Developer Guide or refer to the source code for the HandleIssues AWS Lambda function. To use the AppSync API with an AppSync client, your AWS Identity and Access Management (IAM) role must have the necessary permissions to perform the desired AppSync queries and mutations.

**API**

This solution uses AWS AppSync as its API layer. You can call this GraphQL API directly to create issues or to query for data. The solution provides an AWS AppSync GraphQL endpoint, which allows you to send HTTP POST requests to interact with the GraphQL API. This endpoint is created by AWS AppSync. You can identify this endpoint after the stack is created by navigating to the Outputs tab and locating the value of the GraphQLEndpoint.

When using this API, you must sign AWS requests with Signature Version 4. For more information, refer to Signing AWS requests with Signature Version 4 in the AWS General Reference Guide. This process generates the values needed for the X-Amz-Content-Sha256, X-Amz-Date, and Authorization headers.

Two Issue Management API mutations available in the solution’s APIs are provided: `createIssue` and `updateIssue`. A comprehensive list of queries and mutations for this solution's API is available from the AWS AppSync console. From the APIs page, select ava-api and a list of the solution's APIs is displayed on the Schema page. For more information about the AWS AppSync GraphQL, refer to GraphQL Overview in the AWS AppSync Developer Guide.

![Figure 3: Solution APIs listed on AWS AppSync](image-url)
Note
When sending API requests as an IAM user, this user must have the IAM permissions to perform AWS AppSync actions for that API. Additionally, the specific queries and mutations in the AWS AppSync schema must have @aws_iam as an authorization option for that action.

Issue Management APIs

createIssue

Creates a new Issue with the supplied Event and Site Hierarchy details.

Request syntax:

```plaintext
POST /graphql HTTP/1.1
Host: <VALUE>
X-Amz-Content-Sha256: <VALUE>
X-Amz-Date: <VALUE>
Authorization: <VALUE>
Content-Type: application/json
Content-Length: <VALUE>

mutation SampleCreateIssue {
  createIssue(
    input: {
      id: "<string>",
      siteName: "<string>",
      areaName: "<string>",
      stationName: "<string>",
      deviceName: "<string>",
      processName: "<string>",
      eventId: "<string>",
      eventDescription: "<string>",
      eventType: "<string>",
      issueSource: "<string>",
      priority: "<string>",
      status: "<string>",
      created: "AWSDateTime",
      acknowledged: "AWSDateTime",
      closed: "AWSDateTime",
      acknowledgedTime: "<number>",
      resolutionTime: "<number>",
      createdBy: "<string>",
      additionalDetails: "<string>
    }
  ) {
    id
  },
  variables: {} 
}
```

Request body:

id

The ID of the new issue to be created. If an ID is not supplied, a 128-bit randomly generated UUID will be used.

Type: String

Required: No
siteName
The name of the site for which this issue will be created.
Type: String
Required: Yes

areaName
The name of the area for which this issue will be created.
Type: String
Required: Yes

stationName
The name of the station for which this issue will be created.
Type: String
Required: Yes

deviceName
The name of the Device for which this issue will be created.
Type: string
Required: Yes

processName
The name of the process for which this issue will be created.
Type: String
Required: Yes

eventId
The event ID for an issue.
Type: String
Required: Yes

eventDescription
The description for an event where there is an issue.
Type: String
Required: Yes
eventType
The type of the event where there is an issue.
Type: String
Required: No

issueSource
The source of the issue; values include: webClient, s3File, and device.
Type: String
Required: Yes

priority
The event priority for this issue; values include: low, medium, high, and critical.
Type: String
Required: Yes

status
Status of the issue; values include: open, acknowledged, closed, inprogress, and rejected.
Type: String
Required: Yes

created
Timestamp for when this issue was created, in AWSDateTime format.
Type: String
Required: Yes

acknowledged
Timestamp for when this issue was acknowledged, in AWSDateTime format.
Type: String
Required: Yes

closed
Timestamp for when this issue was closed, in AWSDateTime format.
Type: String
Required: No
acknowledgedTime

   The number of seconds the issue was active before being acknowledged.
   Type: Number
   Required: No

resolutionTime

   The number of seconds the issue was active before being resolved.
   Type: Number
   Required: No

createdBy

   Identifier (such as the email address) of the person or entity creating the issue.
   Type: String
   Required: Yes

additionalDetails

   JSON string providing additional details about the issue, such as anomaly details for issues raised
   from processing Amazon Lookout for Equipment results.
   Type: String
   Required: No

Response syntax:

   HTTP/1.1 200
   {
      data: {
         createIssue: {
            id: "<string>"
         }
      }
   }

Response elements:

id

   The ID of the new issue.
   Type: String

updateIssue

   Updates an existing Issue with the supplied properties.

Request syntax:
POST /graphql HTTP/1.1
Host: <VALUE>
X-Amz-Content-Sha256: <VALUE>
X-Amz-Date: <VALUE>
Authorization: <VALUE>
Content-Type: application/json
Content-Length: <VALUE>

mutation SampleUpdateIssue {
  updateIssue(
    input: {
      id: "<string>",
      siteName: "<string>",
      areaName: "<string>",
      stationName: "<string>",
      deviceName: "<string>",
      processName: "<string>",
      eventId: "<string>",
      eventDescription: "<string>",
      eventType: "<string>",
      issueSource: "<string>",
      priority: "<string>",
      status: "<string>",
      created: "AWSDateTime",
      createdAt: "AWSDateTime",
      acknowledged: "AWSDateTime",
      closed: "AWSDateTime",
      acknowledgedTime: "<number>",
      resolutionTime: "<number>",
      createdBy: "<string>",
      closedBy: "<string>",
      rejectedBy: "<string>",
      acknowledgedBy: "<string>",
      additionalDetails: "<string>",
      expectedVersion: "<number>",
      rootCause: "<string>",
      comment: "<string>"
    }
  ) {
    id
    status
    variables: {}
  }
}

Request body:

id

The ID of the new issue to be created.

Type: String

Required: No

siteName

The name of the site where this issue is created.

Type: String

Required: No
areaName
The name of the area where this issue is created.
Type: String
Required: No

stationName
The name of the station where this issue is created.
Type: String
Required: No

deviceName
The name of the device where this issue is created.
Type: String
Required: No

processName
The name of the process where this issue is created.
Type: String
Required: No

eventId
The ID of the event where there is an issue.
Type: String
Required: Yes

eventDescription
The description of the event where there is an issue.
Type: String
Required: No

eventType
The type of the event where there is an issue.
Type: String
Required: No
issueSource

Source for the issue; values include: webClient, s3File, and device.
Type: String
Required: Yes

priority

The event priority for this issue; values include: low, medium, high, and critical.
Type: String
Required: No

status

Status of the issue; values include: open, acknowledged, closed, inprogress, and rejected.
Type: String
Required: Yes

created

Timestamp for when this issue was created, in AWSDateTime format.
Type: String
Required: No

createdAt

UTC timestamp for when this issue was created, in AWSDateTime format.
Type: String
Required: No

acknowledged

Timestamp for when this issue was acknowledged, in AWSDateTime format.
Type: String
Required: No

closed

Timestamp for when this issue was closed, in AWSDateTime format.
Type: String
Required: No
acknowledgedTime

The number of seconds the issue was active before being acknowledged.

Type: Number
Required: No

resolutionTime

The number of seconds the issue was active before being resolved.

Type: Number
Required: No

createdBy

The identifier (such as an email address) of the person or entity creating the issue.

Type: String
Required: No

closedBy

The identifier (such as an email address) of the person or entity closing the issue.

Type: String
Required: No

rejectedBy

The identifier (such as an email address) of the person or entity rejecting the issue.

Type: String
Required: No

acknowledgedBy

Identifier (i.e., email address) of the person or entity acknowledging the issue.

Type: String
Required: No

additionalDetails

JSON string with providing additional details about the issue, such as anomaly details for issues raised from processing Amazon Lookout for Equipment results.

Type: String
Required: No
expectedVersion

The version of the Issue that is being updated. If this version does not match the latest version, the update will fail.

Type: Number

Required: Yes

rootCause

When closing an issue, the name of the root cause for this issue.

Type: String

Required: No

comment

When closing an issue with a root cause, provides additional details about what caused the issue.

Type: String

Required: No

Response syntax:

```
HTTP/1.1 200
{
  data: {
    updateIssue: {
      id: "<string>",
      status: "<string>"
    }
  }
}
```

Response elements:

id

The ID of the updated issue.

Type: String

status

The new status of the issue.

Type: String

---

Amazon Cognito user groups

The solution uses Amazon Cognito to authenticate users. Authorization to the different user interface components is restricted by the user’s assigned group. As shown in Figure 4, the solution administrator assigns a user to one of the following groups:
• **Admin Group**: Users in this group have access to all menu options, providing them with access to the management, analysis, and client tools, as well as the Observer function.

• **Manager Group**: Users in this group can access the Client, Observer, and Issues Reporting menu options, providing them with access to the analysis and client tools and the Observer function.

• **Engineer Group**: Users in this group can access the Client and Observer options.

• **Associate Group**: Users in this group can access the Client option.

As an administrator you can restrict a user's access to certain sites, processes, and areas so that only information related to the assigned group can be viewed. The solution administrator manages this access through Amazon Cognito user groups to the AWS AppSync GraphQL queries and mutations. Users that are not in the appropriate resolver group cannot query the AWS AppSync schema. For example, the following schema shows a schema.graphql file where only users assigned to the Admin Group have access to the mutations that allow a site to be deleted (deleteSite).

```graphql
type Mutation {
  deleteSite(id: ID!): Site @aws_auth(cognito_groups: ["AdminGroup"])
}
```

If the user calling the deleteSite mutation is not in the AdminGroup, an error will be returned and the request will be blocked. The following code is from `mutation.delete.req.vtl`, the Velocity Template Language (VTL) code that performs the deleteSite request. The authorization is checked at the top and if the user is not in the AdminGroup, the `unauthorized()` utility function is used to block the request.

```vhdl
## Check authorization
#set ($isAllowed = false)
#set ($userGroups = $ctx.identity.claims.get("cognito:groups"))
#set ($allowedGroups = ["AdminGroup"])
#foreach ($userGroup in $userGroups)
#if ($allowedGroups.contains($userGroup))
  #set ($isAllowed = true)
  #break
#end
#end

## Throw authorized if the user is not authorized.
#if ($isAllowed == false)
  $util.unauthorized()
#endif
{
  "version": "2017-02-28",
  "operation": "DeleteItem",
  "key": {
    "id": $util.dynamodb.toDynamoDBJson($ctx.args.id)
  }
}
```
Amazon DynamoDB

This solution uses Amazon DynamoDB to persist factory setup data and store user generated issues. This solution creates the following DynamoDB tables:

- **Data Hierarchy**: Stores information related to a factory’s layout (*Sites, Areas, Processes*, etc.) as well as user *Permissions* and *Root Causes*.
- **Issue**: Stores metadata about the issues that are activated by users.

AWS IoT Core

The web interface communicates with AWS IoT Core to publish messages regarding the issues occurring on the factory floor to an AWS IoT Core topic. Specifically, the web interface uses the AWS Amplify *PubSub category* with AWSIoTProvider, which signs a request according to Signature Version 4. The AWS IoT Core rules engine invokes an AWS Lambda function that processes the message.

The solution creates an AWS IoT Core policy during deployment. When a user accesses the web interface, the appropriate AWS IoT Core policy is assigned an Amazon Cognito identity based on the group that the user belongs to. This policy allows the user to post to the *ava/issues* and *ava/groups/*# AWS IoT topics.

Solution microservices

The Virtual Andon on AWS microservices are a series of AWS Lambda functions that provide the business logic and data access layer for all device operations. Each Lambda function assumes an AWS Identity and Access Management (IAM) role with least privilege access (minimum permissions necessary) to perform its designated functions.

AWS AppSync Lambda resolver microservice

The AppSyncLambdaResolver microservice is used when complex logic is involved in the processing of an AWS AppSync mutation. An AWS Lambda function is invoked to process either the entire mutation or a certain component of it. For example, when creating or updating an event, this microservice is used to manage changes to the solution’s *IssueNotification* Amazon SNS topic after the event has been updated directly with a velocity template language (VTL) template.

Handle issues microservice

The HandleIssues microservice runs every time a message is posted to the *ava/issues* topic in AWS IoT Core or a file is placed in the *DetectedAnomalies* Amazon S3 bucket. This microservice calls the AWS AppSync API to store the issue details in the *issue* Amazon DynamoDB table, and sends a notification to the Amazon Simple Notification Service (Amazon SNS) topic for the event.

Amazon Cognito trigger microservice

This microservice is used only when you have configured a SAML identity provider. To assist with managing users that have logged into the solution’s web interface using a SAML identity provider, a Post
Confirmation Lambda Trigger invokes this microservice to run custom actions for these users. By default, this Lambda function logs only that a user has been created using the Federated SAML access. This function can be extended by choosing to either automatically add users to specific Amazon Cognito user groups or by setting default permissions in the solution. Existing user management capabilities in the web interface exist for federated SAML users if you prefer to manually configure groups and permissions for these users.

**Solution helper microservice**

The SolutionHelper microservice supports the initial solution setup, which includes putting the solution’s web interface resources and configuration into an Amazon Simple Storage Service (Amazon S3) bucket. This microservice also updates the solution when customers deploy a new version of the solution.

**External integrations microservice**

The ExternalIntegrations microservice is an entry point for external systems to create issues in Virtual Andon on AWS. For example, if IoT devices send messages directly to the ava/devices IoT Core topic, this microservice is invoked. Similarly, if you are using Amazon Lookout for Equipment and supply the name of the Amazon S3 bucket where anomaly files will be delivered, this microservice is invoked whenever an anomaly file is added to the bucket. After performing validation, this microservice publishes a message to the ava/issues IoT Core topic where the HandleIssues microservice creates the issue.
Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For more information about security on AWS, visit AWS Cloud Security.

IAM roles

AWS Identity and Access Management (IAM) roles allow customers to assign granular access policies and permissions to services and users on the AWS Cloud. Virtual Andon on AWS creates several IAM roles, including roles that grant the solution's AWS Lambda functions and Amazon Cognito identity pool to access the other AWS services used in this solution.

Amazon CloudFront

This solution deploys a static website hosted in an Amazon Simple Storage Service (Amazon S3) bucket. To help reduce latency and improve security, this solution includes an Amazon CloudFront distribution with an origin access identity, which is a special CloudFront user that helps provide public access to the solution's website bucket contents. For more information, refer to Restricting Access to Amazon S3 Content by Using an Origin Access Identity.

The solution uses the default CloudFront certificate which supports TLS v1.0 only. To use TLS v1.1 or TLS v1.2, you must use a custom SSL certificate instead of the default CloudFront certificate. For more information, refer to How do I configure my CloudFront distribution to use an SSL/TLS certificate.

Amazon S3 buckets

By default, the Amazon S3 buckets deployed by the Virtual Andon on AWS solution are automatically activated with encryption at rest, logging, blocked public access, and access restricted to Amazon CloudFront origin access identity.

Amazon Cognito

Virtual Andon on AWS uses Amazon Cognito to provide secure access (username and password) to its web interface. An admin user is created in a Cognito user pool as part of the solution's deployment. Access to the web interface is restricted to authorized users using an Amazon Cognito identity pool.

SAML identity provider

This solution creates an Amazon Cognito user pool and an identity pool for authentication, authorization, and user management for the solution's web interface. You have the option to add and configure a SAML identity provider (IdP) to the Cognito user pool. The AWS CloudFormation template provides the following parameters so you can set up this security mechanism: Cognito Domain Prefix,
**SAML Provider Name**, and **SAML Provider Metadata Url**. For more information about adding a SAML IdP, refer to *Adding SAML Identity Providers to a User Pool* in the *Amazon Cognito Developer Guide*.

After users initially sign in to Virtual Andon on AWS using SAML IdP, administrators will be able to assign them to groups and set permissions through the web interface. Alternatively, the *Amazon Cognito trigger microservice (p. 17)* can be used to automate the initial configurations of new SAML IdP users.
Considerations

Architecture with all optional resources

This solution includes optional AWS CloudFormation parameters. When these parameters are activated, additional infrastructure, including support for a SAML Identity Provider and data analytics tools, is included in the solution’s architecture. If the bucket name used with Amazon Lookout for Equipment is supplied, the solution will be configured to monitor that bucket for updated files.

Figure 5: Virtual Andon on AWS architecture with optional resources

Figure 5 shows the Virtual Andon on AWS architecture with the optional AWS resources activated. Refer to the Architecture overview (p. 3) section for details about steps 1 through 7.

8. If you are using Lookout for Equipment to monitor your machines, you can supply the name of the Amazon S3 bucket where inference files will be delivered in the Anomaly Detection Output Bucket CloudFormation parameter. This solution can be configured (p. 30) to automatically raise issues if an anomaly is detected.
9. When the **Activate Glue Workflow** CloudFormation parameter is set to **Yes**, an AWS Glue workflow will be created to extract data from DynamoDB to an AWS AWS Glue Data Catalog in Amazon S3. For more information, refer to the *Data Analysis* (p. 4) section.

10. If you would like to use an existing SAML provider as an additional Identity Provider for access to this solution, you can configure the **Cognito Domain Prefix**, **SAML Provider Name**, and **SAML Provider Metadata Url** CloudFormation parameters. For more information, refer to *SAML identity provider* (p. 19).

## Amazon Cognito limits

This solution uses Amazon Cognito user pools to manage users. Amazon Cognito sends an email every time you create a user, change a password, or reset a password. Amazon Cognito **limits** the number of emails sent daily per user pool to 50. For customers who plan to use this solution for a large number of users, we recommend using Amazon Simple Email Service (Amazon SES) for these emails. For more information, refer to *Authorizing Amazon Cognito to Send Amazon SES Email on Your Behalf* in the *Amazon Cognito Developer Guide*.

## Regional deployments

This solution uses AWS AppSync and Amazon Cognito, which are currently available in specific AWS Regions only. Therefore, you must launch this solution in an AWS Region where these AWS services are available. For the most current availability by Region, refer to the *AWS Regional Services List*.

Additionally, Amazon Simple Notification Service (Amazon SNS) supports SMS messaging in specific AWS Regions only. For a list of supported Regions, refer to *Supported Regions and Countries* in the *Amazon SNS Developer Guide*.

**Note**

Effective June 1, 2021, changes have been made that will require manual setup to send SMS messages to US destinations. For more information, refer to *special requirements for sending SMS messages to US destinations* in the *Amazon SNS Developer Guide*.

## Solution updates

Virtual Andon on AWS v3.0 includes breaking changes and cannot be upgraded from previous versions. Updating from version 2.x to version 3.0 requires migrating all your data from the previous deployment to the new deployment (such as data stored in Amazon DynamoDB). Raise questions on the *Issues page* in the GitHub repository.
AWS CloudFormation template

This solution uses AWS CloudFormation to automate the deployment of Virtual Andon on AWS in the AWS Cloud. It includes the following CloudFormation template, which you can download before deployment.

**View Template**

*amazon-virtual-andon.template*: Use this template to launch the Virtual Andon on AWS solution and all associated components. The default configuration deploys Amazon CloudFront, Amazon Simple Storage Service (Amazon S3), Amazon Cognito, AWS AppSync, AWS Lambda, Amazon DynamoDB, Amazon Simple Notification Service, and AWS IoT Core, but you can also customize the template based on your specific network needs.
Automated deployment

Before you launch the automated deployment, review the architecture, configuration, and other considerations in this guide. Follow the step-by-step instructions in this section to configure and deploy the Virtual Andon on AWS solution into your account.

**Time to deploy:** Approximately 15 minutes

Deployment overview

The procedure for deploying this architecture on AWS consists of the following steps. For detailed instructions, follow the links for each step.

**Note**
For information about updating this solution, refer to Solution updates (p. 22) in this guide.

**Step 1. Launch the stack** (p. 24)
- Launch the AWS CloudFormation template into your AWS account.
- Enter a value for the required parameter: **AdministratorEmail**.

**Step 2. Sign in to the web interface** (p. 27)
- Sign in to the web interface using your email address and temporary password.

**Step 3. Add users** (p. 27)
- Add the people in your organization that require access to the web interface.

**Step 4. Add the root causes** (p. 28)
- Add the root causes for events you identify in the solution.

**Step 5. Add site details** (p. 28)
- Add sites and set up the factory details.
- Optional: Configure Amazon Lookout for Equipment
- Optional: Configure IoT devices

**Step 6. Add permissions for users in the Associate Group** (p. 31)
- Add permissions for the users that are in the Associate Group.

---

**Step 1. Launch the stack**

**Important**
This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products.
AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your template and deploy the solution. For more information, refer to the Collection of operational metrics (p. 45) section of this guide.

This automated AWS CloudFormation template deploys Virtual Andon on AWS in the AWS Cloud.

**Note**
You are responsible for the cost of the AWS services used while running this solution. Refer to the Cost (p. 2) section for more details. For full details, refer to the pricing webpage for each AWS service used in this solution.

1. Sign in to the AWS Management Console and use the button below to launch the *amazon-virtual-andon* AWS CloudFormation template.

![Launch Solution](image)

You can also download the template as a starting point for your own implementation.

2. The template launches in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the Region selector in the console navigation bar.

**Note**
This solution uses AWS AppSync and Amazon Cognito, which are currently available in specific AWS Regions only. Therefore, you must launch this solution in an AWS Region where these AWS services are available. For the most current availability by Region, refer to the AWS Regional Services List.

3. On the Create stack page, verify that the correct template URL shows in the Amazon S3 URL text box and choose Next.

4. On the Specify stack details page, assign a name to your solution stack.

5. Under Parameters, review the parameters for the template and modify them as necessary. This solution uses the following default values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdministratorEmail</td>
<td>&lt;Requires input&gt;</td>
<td>Email address for the Virtual Andon on AWS administrator. The Admin receives an SNS message containing the web interface URL and sign in credentials.</td>
</tr>
<tr>
<td>DefaultLanguage</td>
<td>Browser default</td>
<td>Virtual Andon on AWS web interface default language. Default value is “Browser Default” which supports the web browser’s language as a default language.</td>
</tr>
<tr>
<td>LogLevel</td>
<td>ERROR</td>
<td>The logging level for AWS Lambda functions and the solution’s web interface. The default level is set to ERROR,</td>
</tr>
</tbody>
</table>
Virtual Andon on AWS AWS Implementation Guide

Step 1. Launch the stack

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>and additional levels include INFO, WARN, VERBOSE, and DEBUG.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Activate Glue Workflow</strong></td>
<td>No</td>
<td>If set to Yes, the solution runs a data extraction weekly (Monday at 1:00 AM UTC) from DynamoDB to Amazon S3 using an AWS Glue workflow. After the workflow runs, the data from the two data tables: data hierarchy and issues, are exported into an Amazon S3 bucket. The data can then be imported to an analytics tool or queried ad-hoc using Amazon Athena.</td>
</tr>
<tr>
<td><strong>Anomaly Detection Output Bucket</strong></td>
<td>&lt;Optional input&gt;</td>
<td>This parameter is used only with Amazon Lookout for Equipment. Enter the name of the Amazon S3 bucket where anomaly files should be stored. These anomaly files can then be used to automatically create Issues within this solution.</td>
</tr>
<tr>
<td><strong>Cognito Domain Prefix</strong></td>
<td>&lt;Optional input&gt;</td>
<td>This parameter is used only when configuring a third-party SAML identity provider. The prefix to the Amazon Cognito hosted domain name that will be associated with the user pool.</td>
</tr>
<tr>
<td><strong>SAML Provider Name</strong></td>
<td>&lt;Optional input&gt;</td>
<td>This parameter is used only when configuring a third-party SAML identity provider. The identity provider name.</td>
</tr>
<tr>
<td><strong>SAML Provider Metadata Url</strong></td>
<td>&lt;Optional input&gt;</td>
<td>This parameter is used only when configuring a third-party SAML identity provider. Metadata URL for the identity provider details.</td>
</tr>
</tbody>
</table>

6. Choose Next.
7. On the Configure stack options page, choose Next.
8. On the Review page, review and confirm the settings. Check the boxes acknowledging that the template creates AWS Identity and Access Management (IAM) resources and may require an AWS CloudFormation capability.

**Note**
This solution may require an AWS CloudFormation capability: CAPABILITY_AUTO_EXPAND, which is a parameter that supports the use of macros. For information about this AWS CloudFormation capability, refer to CreateStack in the AWS CloudFormation API Reference.
9. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a **CREATE_COMPLETE** status in approximately 15 minutes.

**Note**
You will receive an email containing your login information before the stack creation process is completed. Wait until you receive a **CREATE_COMPLETE** status before accessing and signing in to the Virtual Andon on AWS web interface.

---

**Step 2. Sign in to the web interface**

After the AWS CloudFormation stack creation completes, the resources for the web interface are deployed. Use the email you received to obtain the URL for the web interface and your admin credentials, which include a temporary password.

1. Open the email and select the URL link.

2. On the **Virtual Andon on AWS sign in** page, enter your admin email address and temporary password.

3. On the **Change Password** page, enter a new password.

   **Note**
   Password requirements—minimum of eight characters, requiring at least one upper case character, one number, and one symbol.

4. Optional: On the **Account recovery** page, select **E-Mail** to receive a code to verify your contact information. You can skip the account recovery setup.

After you sign in to the web interface, follow the remaining steps to set up the factory details, including adding users, creating the root causes, and other information.

---

**Step 3. Add users**

Use the following procedure to add the users in your organization that require access to the web interface. These users include additional administrators for this solution, managers that analyze metrics-related issues, engineers that troubleshoot issues, and other users.

1. From the **Virtual Andon on AWS** homepage, choose **Users**.

2. You can manually create users in the web interface, or use the provided CSV template to add multiple users.

   - Use the following steps to manually create a new user:
     a. Choose **Add User**.
     b. Enter the user’s email address to receive automated notifications from the solution.
     c. Under **Groups**, check the appropriate group(s) for this user.
     d. Choose **Add**.
     e. Repeat these steps to continue adding users manually.

   - To add multiple users at once, take the following steps:
     a. Choose **Download CSV**.
     b. Open the CSV file and enter the following information:
        - For username, enter the email addresses for the users requiring access to the web interface.
Step 4. Add the root causes

Root causes link to events. An event can be initiated by one or more root causes and administrators can define common root causes for events using the web interface. Therefore, root causes must be defined first before they can be linked to root causes. From the Root Causes page, use the following procedure to either manually enter root causes one at a time using the web interface, or use the included CSV file to upload multiple root causes.

1. From the Virtual Andon on AWS homepage, choose Root Causes.
2. Choose one of the following options to create the root causes:
   - Use the following steps to manually create a root cause:
     a. Choose Add Root Cause.
     b. In the Add Root Cause dialog box, enter a root cause and choose Add.
     c. Repeat these steps to continue adding root causes manually.
   - To use the included CSV file, take the following steps:
     a. Choose Download CSV.
     b. Enter the root causes in the CSV file. Enter only one root cause in each row.
     c. Save the CSV file.
     d. Choose Upload CSV, select the CSV file, and choose Upload.

Step 5. Add site details

The solution administrator adds the site details for the solution to monitor. Use the following procedure to add site details.

1. From the Virtual Andon on AWS homepage, choose Sites.
2. From the Sites page, choose Add Site.
3. In the Site Registration dialog box, enter the Site Name and Site Description.
4. Choose Register.

After a site is created in the web interface, you can add the necessary details. Use the following procedure to add Areas, Stations, Devices, Processes, and Events. The following details are required: at least one process and station in an area and at least one device in each station for each area you identify.
Virtual Andon on AWS AWS Implementation Guide
Step 5. Add site details

1. From the Sites page, identify the site to add details to and choose Detail.
2. From the Areas page, choose Add Area.
3. In the Area Registration dialog box, enter the Area Name and Area Description and choose Register.

   **Note**
   You can continue to add areas from the Areas page.
4. From the Areas page, in the section displaying the name of the area you created, choose Stations.
5. On the Stations page, choose Add Station.
6. In the Station Registration dialog box, enter the Station Name and Station Description and choose Register.

   **Note**
   You can continue to add stations from the Stations page.
7. From the Stations page, in the Station section, choose Details.
9. In the Device Registration dialog box, enter the Device Name and Device Description.
10. Optionally, enter the Device Alias.
11. Choose Register.

   **Note**
   You can continue to add devices from the Devices page.
12. To add a process, select the name of the area that you created from the navigation bar.
13. From the Areas page, in the section displaying the name of the area, choose Processes.
15. In the Process Registration dialog box, enter the Process Name and Process Description and choose Register.

   **Note**
   You can continue to add processes from the Processes page.
16. To add an event to the process you just created, locate the name of the process and choose Detail.
17. On the Events page, choose Add Event.
18. In the Event Registration dialog box, enter the following required information:

   a. Event Name
   b. Event Description
   c. Event Priority
   d. Optionally, enter a group email address, SMS number, Event Type, and, if available, select the root causes for this event.

      **Note**
      You can enter multiple SMS numbers and email addresses using a comma-separated list.
   e. Optionally, insert an image to be associated with the event.
19. Choose Save.

   **Note**
   You can continue to add events from the Events page.

You can add sub events to an event after it is created. For guidance to add sub events and to edit the site details, refer to Solution web interface (p. 34).
Optional: Configure Amazon Lookout for Equipment

If you are integrating Amazon Lookout for Equipment, you can create an automated event in the solution’s web console by taking the following steps.

1. Follow Step 5 (p. 28) for creating Sites, Areas, and Processes.
2. To add an event to a process, locate the name of the process and choose Detail.
3. On the Events page, choose Add Event.
4. In the Event Registration dialog box, enter the following required information:
   a. Enter an Event Name.
   b. Enter an Event Description.
   c. For Event Type, enter automated as the value.
   d. Select an Event Priority.
   e. Optionally, enter a group email address, SMS number, and, if available, select the root causes for this event.
   f. Optionally, insert an image to be associated with the event
6. In the Device Registration dialog box, enter the following required information:
   a. Enter a device name.
   b. Enter a description for your device.
   c. For Device Alias, enter the name of the machine as it will appear in the diagnostic data reported by Lookout for Equipment. Do not include a specific sensor name; only the name of the machine is required.

Optional: Configure IoT devices

The following messages code sample shows an example message setup that can be sent to the ava/devices IoT Core topic.

```json
{
   "messages": [
      {
         "name": "site/area/process/machine/status",
         "timestamp": "2021-03-31 00:15:28.487000+00:00",
         "quality": "GOOD",
         "value": "down"
      }
   ]
}
```

Once configured, the IoT device invokes an AWS Lambda function, which takes the following actions:

1. Retrieves the last element (most recent) from the messages array.
2. Parses the name field to extract the machine and tag names.

   The name field is split by a delimiter (forward slash) and the final value becomes the tag name. The remaining name string is used as the device name. For example, using the code sample:
   - The device name would be site/area/process/machine
   - The tag name would be status
3. The tag value is taken from the message’s value property. In the code sample, down is the tag value.
To ensure your IoT devices are properly connected to Virtual Andon on AWS, take the following steps:

1. Follow Step 5 (p. 28) for creating Sites, Areas, and Stations.
2. From the Stations page, in the Station section, choose Details.
4. In the Device Registration dialog box, enter the Device Name and Device Description.
5. Use the IoT device name as the Device Alias. For example, in the messages code sample, you would enter site/area/process/machine in the Device Alias field in Amazon Virtual Andon.

To associate a Virtual Andon on AWS Event with a specific tag and value, use the tag name and value separated by an underscore as the Event Alias when creating the new event. In the messages code sample, the Event Alias is status\_down.

If an Event and Device are matched, an Issue is raised in Amazon Virtual Andon.

**Note**
The Device and Event must belong to the same Process.

## Step 6. Add permissions for users in the Associate Group

Use the following procedure to add permissions for users in the Associate Group.
1. From the Virtual Andon on AWS homepage, choose Permissions.
2. Choose Add Permission.
3. On the Permissions / Permissions Setting page, select the user’s email.
4. From the list of sites, select the checkbox next to the site name. A list of Areas available for that site displays.
5. For each Area, select the checkbox next to the processes, stations, and devices to grant access permission to the user.

After the permission is set, the user can access the site information from the Client page. For information about editing or removing a user’s permission in the Associate Group, refer to Solution web interface (p. 34).
Additional resources

AWS services

- AWS CloudFormation
- AWS IoT Core
- AWS Lambda
- Amazon DynamoDB
- Amazon Simple Notification Service
- Amazon Lookout for Equipment
- Amazon Simple Storage Service
- Amazon Cognito
- Amazon CloudFront
- AWS AppSync
- AWS Glue
- Amazon Athena

Related AWS Solutions

- Machine to Cloud Connectivity Framework
- Smart Product Solution
- Predictive Maintenance Using Machine Learning
Solution web interface

The Virtual Andon on AWS solution deploys a web interface that provides management, client, and analysis tools, as well as an observer function.

Management pages

The web interface provides the following management pages: Sites, Users, Permissions, and Root Causes. These pages are accessible only to users assigned to the Admin Group.

- **Sites page**: Registers and manages the factory details
- **Users page**: Manages users and assign them to one or more groups
- **Root Causes page**: Creates the root causes for events and issues
- **Permissions page**: Sets up the permissions for users in the Associate Group

Sites page

Use the Sites page to register and manage the sites that the solution monitors. The solution is able to monitor multiple sites. In order for the solution to monitor a site, the following site information is required:

- **Areas**: The area within the site. For example, Floor 1, Floor 2, East, and West.
- **Processes**: The process in a given area. For example, inbound, outbound, and packaging.
  - **Events**: Events that can occur within a given process and area. For example, equipment issues and scanner errors. When creating an event, the administrator can add description details, an email address to send notifications when an event occurs (such as an engineer), associate an image with that event for easier identification on the Client view, and identify the root causes.
  - **Sub Events**: Each event can have multiple sub events. For example, a packaging event may contain sub events identifying the size of the shipping box that is low in inventory, such as large, medium, and small.
- **Stations**: The station in the site and area where one or more devices are installed.
- **Devices**: The devices deployed in the station. You can enter multiple devices for each station.

For information to set up a new site, refer to Step 5. Add site details (p. 28). Use the following procedure to edit an existing site.

1. Sign in to the Virtual Andon on AWS web interface.
2. Choose **Sites**.
3. On the **Sites** page, identify the site you want to edit and choose **Detail**.

   **Tip**
   You can delete a site and all associated details by choosing **Delete**.

On the **Areas** page, you can take the following actions:
• Add a new area (for information to set up a new area, refer to Step 5. Add site details (p. 28)).
• Edit the area's station information.
• Edit the processes for the area.
• Delete an area.

If you have a large number of areas for a site, use the search tool to locate the specific area that you want to edit.

**Edit the area's station information**

1. On the **Areas** page, identify the area you want to edit and choose **Stations**.
2. On the **Stations** page, identify the station you want to edit and choose **Detail**.
3. On the **Devices** page, you can take the following actions:
   • Add a new device by choosing **Add Device**.
     
     **Note**
     In the **Device Registration** dialog box, enter the **Device Name** and **Device Description** and choose **Register**.
   • Search for a device using the search tool.
   • Delete a device you no longer need to monitor.

**Add and manage sub events for an event**

1. On the **Events** page, identify the process you want to edit and choose **Edit**.
2. On the **Edit Event** page, choose **Manage Sub Events**.
3. In the **Manage Sub Events** dialog box, add your sub events.
4. Choose **Save**.

If you have created sub events, you can manage them by choosing **Manage Sub Events** and taking the following actions:

• Add a second level sub event.
• Delete a sub event.
• Add an image to sub events and second level sub events.

**Users page**

For information to set up a new user, refer to **Step 3. Add users (p. 27)**. Use the following procedure to edit the information for an existing user.

1. Sign in to the Virtual Andon on AWS web interface.
2. Choose **Users**.
3. Locate the user and choose **Edit**.
   
   **Tip**
   Use the search tool if you have a large list of users.
4. In the **Edit User** dialog box, you can edit the emails address and change the group affiliation.
5. Choose **Save**.
Optionally, you can remove the user by choosing **Delete**.

**Root causes page**

Admins can manage root causes to events. For information to set up new root causes, refer to *Step 4. Add the root causes (p. 28)*. Use the following procedure to delete existing root causes.

1. Sign in to the Virtual Andon on AWS web interface.
2. Choose **Root Causes**.
3. Locate the root cause and choose **Delete**.
   
   **Tip**
   
   Use the search tool if you have a large list of root causes.

**Permissions page**

Admins can manage permission for users in the Associate Group. Using this page, admins can change the sites, areas, stations, processes, and devices that a user can access. For information to set up new permissions, refer to *Step 6. Add permissions for users in the Associate Group (p. 31)*.

Use the following procedure to edit permissions for existing users.

1. Sign in to the Virtual Andon on AWS web interface.
2. Choose **Permissions**.
3. Locate the user and choose **Edit**.
   
   **Tip**
   
   Use the search tool if you have a large list of users.
4. On the **Permissions Setting** page, you can activate or deactivate the following options by selecting the checkbox:
   
   - The sites
   - The areas for a site
   - The processes, stations, and devices for an area

5. Choose **Save**.

Optionally, you can remove the user by choosing **Delete**.

**Client page**

When an issue occurs on the factory floor, users access the Client page to record the issue in the solution, which can then notify the appropriate personnel for troubleshooting and resolution support. Users in the Admin, Engineer, Manager, and Associate groups can access the Client page. To access events related to a particular process or station, the following site details must be selected: Site Name, Area Name, Process Name, Station Name, and Device Name. The ID of each corresponding site detail is added to the URL's query string to allow specific configurations to be bookmarked.

The events are displayed as text boxes that represent potential issues that can occur with the selected device. Each box contains the event name, description, and the image if one was provided. These text boxes display a particular color based on one of the following statuses:

- **No issue**: The event text box displays a gray color when there is no issue.
• **Open Issue:** The event text box changes to red when a user selects it to identify an issue. Once selected, the web interface synchronizes this change to all the other pages that contains this event. If a point-of-contact is provided for the event, a notification is sent.

• **Acknowledged Issue:** The text box changes to yellow when the issue is acknowledged by a user from the Observer page.

• **Closed or Rejected Issue:** The text box changes back to its original (gray) state when a user closes or rejects the issue from the Observer page.

Refer to Figure 8 for an example of the Client page displaying issue statuses. A scanner issue is shown as an open issue and denoted in red. An equipment issue is shown as acknowledged as denoted in yellow.

![Figure 8: Client console issue status](image)

**Observer page**

Engineers and managers can view issues occurring on the factory floor in real-time using the Observer page. The Observer page provides engineers and managers a live view of all open issues in a selected site, or in a specific area within a site. Additionally, they can acknowledge, close, and reject issues. The selected site and area ID are saved in the URL as a query string in order to allow for bookmarking of a specific configuration.

When engineers close issues, they can choose one of the pre-defined root causes of the event if the event has root causes attached. Once a root cause is chosen, they will also have the option to add a comment.

Refer to Figure 9 for an example of the Observer page displaying issue statuses.

![Figure 9: Live view showing issue statuses](image)
Data analytics

Issues reporting

Users assigned to the Admin and Manager groups can view historical information about issues that have occurred from the Issues Reporting page. The top section shows aggregated statistics for the past 24 hours, including total number of issues, breakdowns by current status (Open/Acknowledged/Closed), and number of issues opened in the past three hours. A log of individual issues can be searched by selecting a site, area, and date range. This data can then be downloaded as a CSV file.

AWS Glue data export

This solution provides the flexibility to export the historical data that is stored in Amazon DynamoDB to an Amazon S3 bucket, where it can then be queried directly using Amazon Athena or used as input in your own BI tool. You can activate this feature when you launch the AWS CloudFormation stack by changing the Activate Glue Workflow CloudFormation parameter to Yes.

By default, AWS Glue workflow runs the data extraction every Monday at 1:00 AM UTC. The extracted data is stored in Amazon Athena tables. Use the following steps to access this data.

1. Sign in to the Amazon Athena console.
2. Choose Query Editor.
3. In the Editor tab, under Data, make the following selections:
   - Under Data Source, access the drop down menu and select AwsDataSource.
   - Under Database, access the drop down menu and select amazon-virtual-andon-glue-database.

Under Tables, two new tables display: one for the solution’s data hierarchy, which contains data on your registered Sites, Areas, Processes, Events, and other factory information. The second table will contain a record of each issue that was raised with Virtual Andon on AWS.

The following sample query can be used to retrieve a day-over-day count of the number of issues that have been opened, by priority level.
SELECT split_part(createdat, 'T', 1) as day, priority, count(1) as num_issues
FROM "amazon-virtual-andon-glue-database"."<your-issues-table>"
where sitename = '<your-site-name>'
group by 1,2
order by 1,2

Figure 11: Query the data for issues in Amazon Athena
Troubleshooting

Common errors

Access denied

If you receive an access denied error with a 307-redirect to the Amazon Simple Storage Service (Amazon S3) bucket URL in a non-US Region, verify that the web interface is accessed using only Amazon CloudFront. For more information, refer to Temporary Request Redirection in the Amazon Simple Storage Service Developer Guide and the article about Access Denied errors in the AWS Premium Support Knowledge Center.

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>0190E084E385D7D5</RequestId>
  <HostId>
    csOEhnlOLv7yCEKxVzBuT0aLaMM0fY8IRO25rmijF2Tbu3EU85gGPQjrI9VSWnmQAMhtggKvxmlFI=
  </HostId>
</Error>
```

Resolution

Wait for the DNS entries to propagate.

A user cannot access the web interface

After the solution administrator creates the user and the user is added to the Amazon Cognito user pool, the user receives an email message with the sign in information. If sign in is successful but the menu options Client, Sites, or Observer are not shown, they may not have been assigned to a group.

Resolution

There are two resolutions:

1. An AWS account administrator must navigate to the Amazon Cognito user pool and assign the user the required permissions and assign the user to the correct groups.
2. The solution administrator can edit the user profile in the web interface and select the appropriate group(s) for the user.

User permission issue

If a user is assigned to the Associate Group only, the user must have permissions to access events on the Client page. However, if the permission was not set correctly, the user will not be able to view any events. In this case, the solution administrator must verify whether the correct permission was provided to the user.

Resolution
Verify that the user is assigned to the Associate Group. In addition, verify that a site contains the required details including areas, processes, stations, and devices. If any type of information is missing, users in the Associate Group cannot view events.

**The solution’s web interface does not support your web browser language as the default language**

Starting with version 2.1, the Virtual Andon on AWS solution supports seven languages: German, English, Spanish, French, Japanese, Korean, and simplified Chinese. If you keep your browser default set to the `DefaultLanguage` parameter when you launch the solution, it detects the web browser’s language. However, if your web browser’s language is not supported, the default web interface language is set to English.
AWS AppSync authorization

AWS AppSync authorization enforces OpenID Connect (OIDC) tokens provided by Amazon Cognito user pools. The application leverages the users and groups in your user pools and associates them with GraphQL fields and operations for controlling access.

When using Amazon Cognito user pools, you can create groups for users. This information is encoded in a JSON web token (JWT) that your application sends to AWS AppSync in an authorization header while sending GraphQL operations. You can set up the authorization in AWS AppSync resolvers to control which groups can run queries.

The following example shows the AWS AppSync resolver, which allows the admin group to get the result:

```graphql
## Check authorization
#set ($isAllowed = false)
#set ($userGroups = $ctx.identity.claims.get("cognito:groups"))
#set ($allowedGroups = ["AdminGroup"])
#foreach ($userGroup in $userGroups)
#if ($allowedGroups.contains($userGroup))
#set ($isAllowed = true)
#break
#end
#end

## Throw authorized if the user is not authorized.
#if ($isAllowed == false)
$util.unauthorized()
#end

{
  "version": "2017-02-28",
  "operation": "Scan",
  #if( $ctx.args.nextToken )
  "nextToken": "$ctx.args.nextToken",
  #end
  "limit": $util.defaultIfNull($ctx.args.limit, 50)
}
```
Uninstall the solution

You can uninstall the Virtual Andon on AWS solution using the AWS Management Console or the AWS Command Line Interface (AWS CLI). However, the Amazon Cognito user pool, Amazon Simple Storage Service (Amazon S3) buckets, and the issue Amazon DynamoDB table must be manually deleted.

Using the AWS Management Console

1. Sign in to the AWS CloudFormation console.
2. On the Stacks page, select the solution stack.
3. Choose Delete.

Using AWS CLI

Determine whether AWS CLI is available in your environment. For installation instructions, refer to What Is the AWS Command Line Interface in the AWS CLI User Guide. After confirming the AWS CLI is available, run the following command.

```
# aws cloudformation delete-stack --stack-name <cloudformation-stack-name>
```

Deleting the Amazon Cognito user pool

Use the following procedure to delete the Amazon Cognito user pool:

1. Sign in to the Amazon Cognito console to access the User Pools tab.
2. Choose the User Pool named ava-userpool.
3. On the ava-userpool page, choose Delete pool.

Deleting the Amazon S3 buckets

The solution is configured to retain the Amazon S3 buckets if you decide to delete the AWS CloudFormation stack to prevent against accidental data loss. After uninstalling the solution, you can manually delete these buckets if you do not need to retain the data. Use the following procedure to delete the Amazon S3 buckets.

1. Sign in to the Amazon S3 console.
2. Choose Buckets from the left navigation pane.
3. Locate the <stack-name> S3 buckets.
4. Select one of the S3 buckets and choose Delete.
Deleting the Amazon DynamoDB tables

Use the following procedure to delete the Amazon DynamoDB issue table.

1. Sign in to the Amazon DynamoDB console.
2. Choose Tables from the left navigation pane.
3. Select the issue Amazon DynamoDB table and choose Delete table.

Repeat the steps until you have deleted all the <stack-name> S3 buckets.

To delete the S3 bucket using AWS CLI, run the following command:

```bash
$ aws s3 rb s3://<bucket-name> --force
```
Collection of operational metrics

This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When activated, the following information is collected:

- **Solution ID**: The AWS solution identifier
- **Unique ID (UUID)**: Randomly generated, unique identifier for each solution deployment
- **Timestamp**: Data-collection timestamp
- **Resource**: The created resource or visited page
- **Region**: The AWS Region where the resource is created
- **Version**: The deployed solution version

AWS owns the data gathered through this survey. Data collection is subject to the [AWS Privacy Policy](https://aws.amazon.com/privacy/). To opt out of this feature, complete the following steps before launching the AWS CloudFormation template.

1. Download the [AWS CloudFormation template](https://aws.amazon.com/cloudformation/)
to your local hard drive.
2. Open the AWS CloudFormation template with a text editor.
3. Modify the AWS CloudFormation template mapping section from:

   ```
   Solution:
   Config:
       AnonymousUsage: "Yes"
   ```

   to

   ```
   Solution:
   Config:
       AnonymousUsage: "No"
   ```

5. Select **Create stack**.
6. On the **Create stack** page, **Specify template** section, select **Upload a template file**.
7. Under **Upload a template file**, choose **Choose file** and select the edited template from your local drive.
8. Choose **Next** and follow the steps in **Step 1. Launch the stack (p. 24)** in the Automated deployment section of this guide.
Source code

Visit our GitHub repository to download the templates and scripts for this solution, and to share your customizations with others.
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2019</td>
<td>Initial version</td>
</tr>
<tr>
<td>July 2020</td>
<td>Release version 2.0.0: changed UI to bootstrap 4; added user, permission, and root cause management pages; removed AWS CodePipeline deployment; for more information, refer to the CHANGELOG.md file in the GitHub repository.</td>
</tr>
<tr>
<td>August 2020</td>
<td>Release version 2.1.0: added multi language support; for more information, refer to the CHANGELOG.md file in the GitHub repository.</td>
</tr>
<tr>
<td>July 2021</td>
<td>Release version 2.2.0: added the following capabilities - create an issue in Amazon S3 using JSON, upload an image associated with an event, add a comment when closing an issue, access all the issues related to a site, and change the URL structure to allow for bookmarking; for more information, refer to the CHANGELOG.md file in the GitHub repository.</td>
</tr>
<tr>
<td>October 2021</td>
<td>Release version 3.0.0: used the AWS Cloud Development Kit (CDK) to create the AWS CloudFormation template; added the option to export the solution's DynamoDB table data to Amazon S3 for in-depth data analysis; added the ability to enter nested “sub events” after creating events; consolidated previous Metrics &amp; History pages into the new Issue Reporting page; added editing option for closed issues for Root Cause and Comments; added option to subscribe multiple email addresses and/or phone numbers to Events for Amazon SNS notifications; added the option to capture the users who create, acknowledge, and close issues so they can be viewed in the Issue Reporting screen. For more information, refer to the CHANGELOG.md file in the GitHub repository.</td>
</tr>
</tbody>
</table>
Contributors

- Nimay Mehta
- Garvit Singh
- Beomseok Lee
- Eric Quinones
- George Lenz
Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Amazon Virtual Andon is licensed under the terms of the Apache License Version 2.0 available at The Apache Software Foundation.