Amazon Virtual Andon

AWS Implementation Guide

Nimay Mehta

Garvit Singh

Beomseok Lee

November 2019

Last Updated: August 2020 (refer to revisions)

Contents

Overview ... 4
Cost ... 4
Architecture overview ... 5
Solution components ... 6
Web interface ... 6
AWS AppSync ... 7
Amazon Cognito user groups ... 7
Amazon DynamoDB ... 9
AWS IoT Core ... 9
Solution microservices ... 9
Considerations ... 10
Amazon Cognito limits ... 10
Regional deployments ... 10
AWS CloudFormation template ... 11
Automated deployment ... 11
Deployment overview ... 11
Step 1. Launch the stack ... 12
Step 2. Sign in to the web interface ... 13
Step 3. Add users ... 14
Step 4. Add the root causes ... 15
Step 5. Add site details ... 15
Step 6. Add permissions for users in the Associate Group ... 17
Security ... 17
IAM roles ... 18
Amazon CloudFront ... 18
Amazon S3 buckets ... 18
Additional resources ... 19
Appendix A: Solution web interface ... 19
Management pages ... 19
Client page ... 22

Observer page 23
Analysis page 24
Appendix B: Troubleshooting 25
Common errors 25
Appendix C: System integration 26
Appendix D: AWS AppSync authorization 27
Appendix E: Migrate from solution version 1 to version 2 28
Appendix F: Uninstall the solution 30
Using the AWS Management Console 30
Using AWS CLI 30
Deleting the Amazon S3 buckets 31
Deleting the Amazon DynamoDB tables 31
Deleting the Amazon SNS topics 31
Appendix G: Collection of operational metrics 32
Source code 33
Document revisions 33

About this guide

This implementation guide discusses architectural considerations and configuration steps for deploying Amazon Virtual Andon 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.

Overview

Andon is a lean manufacturing term referring to a system that notifies management, maintenance, and other workers of a quality or process problem. Traditional Andon systems enable a machine or its operator to activate an alert (visual or audible) at a particular workstation. Factory floor workers identify stations that require assistance by following the light or sound before investigating the incident, and depending on the nature of the issue to resolve, contact the relevant engineer. These systems can be expensive and complicated to deploy because they require additional electrical hardware installation, and they lack modern capabilities, such as the ability to issue targeted notifications and track and archive incidents and root causes.

To help simplify monitoring manufacturing workstations, devices, and events, Amazon Web Services (AWS) offers the Amazon Virtual Andon solution. This solution provides a scalable Andon system to help optimize processes, support the transition to predictive maintenance, and prevent future 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 in real-time. This solution is fully customizable and enables users to update the solution in real-time as issues arise.

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

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 the date of publication, the cost for running this solution with default settings in the US East (N. Virginia) Region is approximately **$8.98 per month**. The cost estimate assumes the following factors:

- 1 GB of Amazon DynamoDB data storage
- One million DynamoDB write capacity units using the On-Demand capacity mode
- One million DynamoDB read capacity units using the On-Demand capacity mode
- One million messages that are transported to the AWS IoT core
- One million rules that are triggered at the AWS IoT core
- One million AWS AppSync query and data modification operations

- One million AWS AppSync real-time updates
- One million minutes of connection time to AWS AppSync

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.

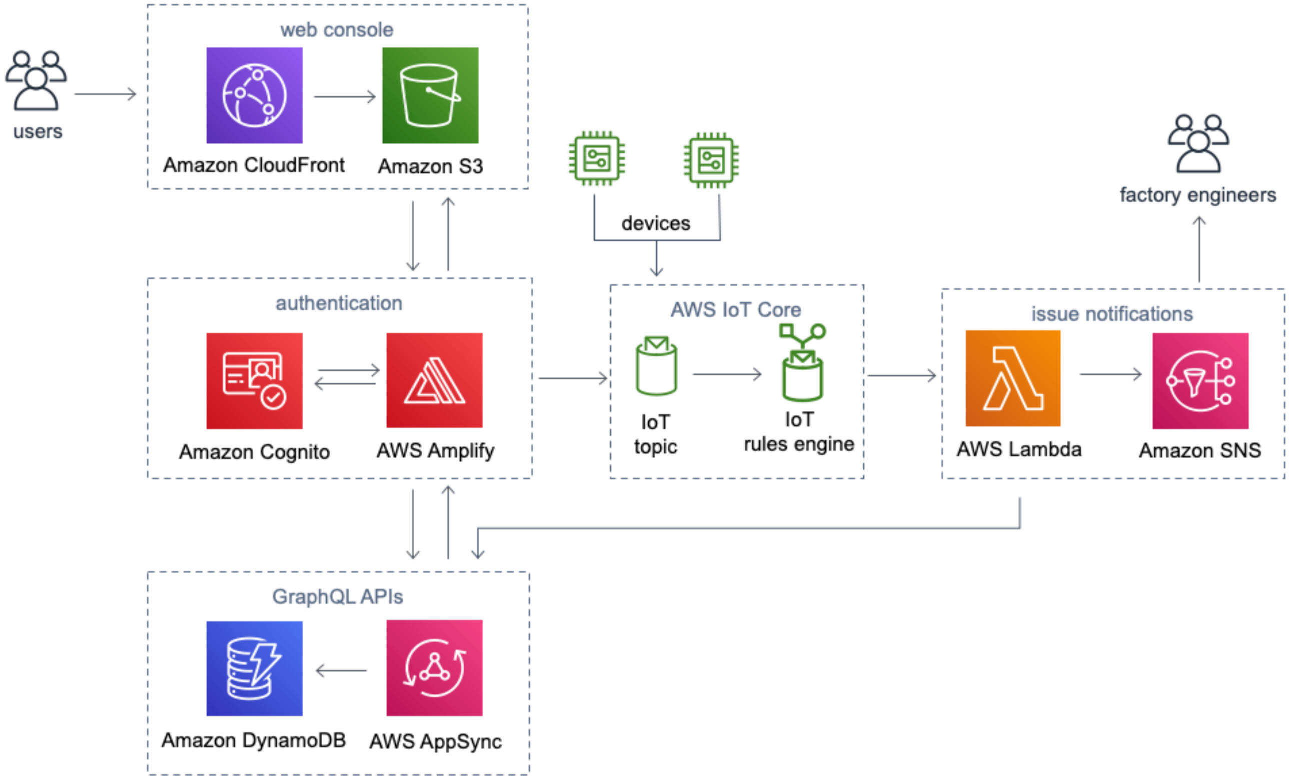


Figure 1: Amazon Virtual Andon architecture on AWS

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. AWS AppSync GraphQL APIs and AWS Amplify power the web interface. An Amazon Cognito user pool enables this solution's administrators to register users and groups using the web interface. Amazon DynamoDB tables store the factory data.

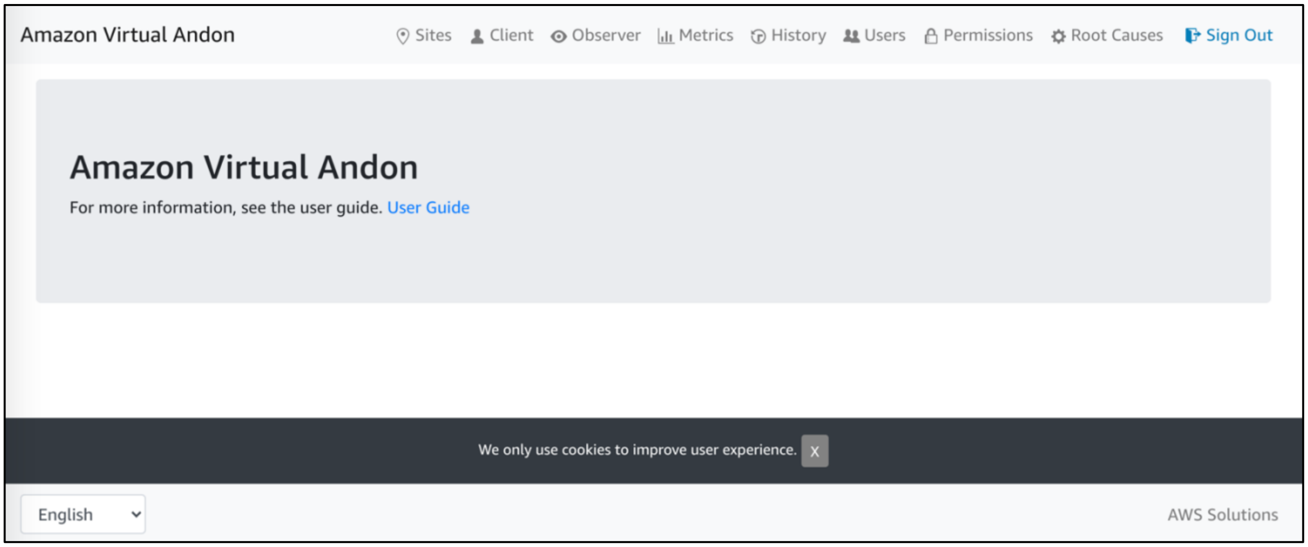
An AWS IoT rule engine helps users monitor manufacturing workstations or devices for events, and then routes the event to the correct engineer for resolution in real-time.

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.

Solution components

Web interface

The Amazon Virtual Andon 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.



Amazon Virtual Andon

For more information, see the user guide. User Guide

We only use cookies to improve user experience.

Figure 2: Amazon Virtual Andon web interface

As shown in Figure 2, the web interface provides the following menu options: Sites, Client, Observer, Metrics, History, 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), 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:** These tools are provided in the Metrics and History menu options. Users assigned to the Admin and Manager groups can view the historical information about issues that have occurred over the last seven days.

- **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.

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

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. For more information about the web interface, refer to Appendix A.

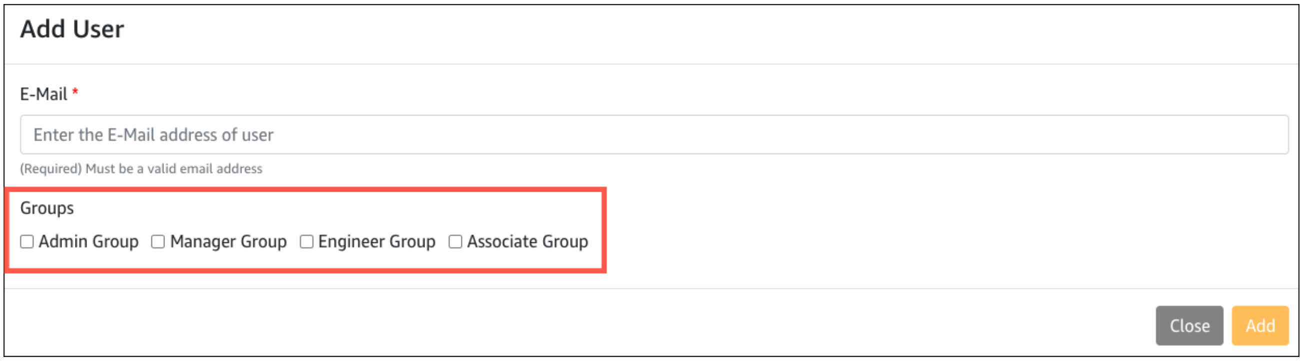
AWS AppSync

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.

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 3, 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, Metrics, and History 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.



Add User

E-Mail *

Enter the E-Mail address of user

(Required) Must be a valid email address

Groups

□ Admin Group □ Manager Group □ Engineer Group □ Associate Group

Figure 3: Web interface Add User page

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.

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

The following schema example shows a `mutation.delete.req.vtl` file where an error message generates if the request does not originate from a user in the Admin Group.

```
## 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": "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:

- **Site:** Stores the Sites metadata
- **Area:** Stores the Areas metadata for the areas in each site
- **Process:** Stores the Processes metadata for each area
- **Event:** Stores metadata for the events that are likely to occur in each process
- **Station:** Stores Stations metadata for each area of a site
- **Device:** Stores Devices metadata for each station
- **Issue:** Stores metadata about the issues that are triggered by users
- **Permission:** Stores Permissions metadata specifically for the Associate Group
- **Root Cause:** Stores the root causes for events that are entered by users in the Admin Group

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 triggers 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 Amazon Virtual Andon 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.

Handle issues microservice

The `handle issues` microservice triggers every time a message is posted to the `ava/issues` topic in AWS IoT Core. This 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.

Custom resource microservice

The `custom Resource` 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.

Considerations

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 AWS service offerings by Region.

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*.

AWS CloudFormation template

This solution uses AWS CloudFormation to automate the deployment of Amazon Virtual Andon 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 Amazon Virtual Andon 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 Amazon Virtual Andon 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.

Step 1. Launch the stack

- 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

- Sign in to the web interface using your email address and temporary password.

Step 3. Add users

- Add the people in your organization that require access to the web interface.

Step 4. Add the root causes

- Add the root causes for events you identify in the solution.

Step 5. Add site details

- Add sites and set up the factory details.

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

- Add permissions for the users that are in the Associate Group.

Step 1. Launch the stack

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

> **Note**: You are responsible for the cost of the AWS services used while running this solution. Refer to the Cost 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 to the right to launch the `amazon-virtual-andon` AWS CloudFormation template.

   Launch Solution

   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 AWS service offerings by Region.

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.

Parameter	Default	Description
AdministratorEmail	*<Requires input>*	Email address for the Amazon Virtual Andon administrator. The Admin receives an SNS message containing the web interface URL and sign in credentials.

Parameter	Default	Description
DefaultLanguage	*Browser default*	The default language used in the solution's web interface. The value is set to the web browser's default language.

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 the CREATE_COMPLETE status before accessing and signing in to the Amazon Virtual Andon 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 **Amazon Virtual Andon 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 **Amazon Virtual Andon** 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.
        - For groups, enter the name of the group(s) for each user in the following format: AdminGroup, ManagerGroup, EngineerGroup, or AssociateGroup.

        > **Note:** If a user belongs to more than one group, use a comma to separate the group names.

        - **Save** the CSV file.

c. In the web interface, choose **Upload CSV**, select the appropriate CSV file, and choose **Upload**. The web interface adds the users identified in the CSV file automatically.

> **Note:** Because users can be assigned to more than one group, a user inherits the permissions of the group with the highest access level. After a user is added to a group, they receive an email with a temporary password to sign in to the web interface. For information about groups, refer to Amazon Cognito User Groups.

Step 4. Add the root causes

Root causes link to events. An event can be triggered 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 **Amazon Virtual Andon** 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 **Amazon Virtual Andon** 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.

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**.
8. On the **Devices** page, choose **Add Device**.
9. In the **Device Registration** dialog box, enter the **Device Name** and **Device Description** and choose **Register**.

> **Note:** You can continue to add devices from the **Devices** page.

10. To add a process, select the name of the area that you created from the navigation bar.
11. From the **Areas** page, in the section displaying the name of the area, choose **Processes**.
12. Choose **Add Process**.
13. 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.

14. To add an event to the process you just created, locate the name of the process and choose **Detail**.
15. On the **Events** page, choose **Add Event**.
16. 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 select the root causes for this event.
17. Choose **Register**.

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

For guidance to edit the site details, refer to Appendix A.

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 **Amazon Virtual Andon** 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 Appendix A.

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 the AWS Security Center.

IAM roles

AWS Identity and Access Management (IAM) roles enable customers to assign granular access policies and permissions to services and users on the AWS Cloud. Amazon Virtual Andon 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 Amazon Virtual Andon solution are automatically enabled with encryption at rest, logging, blocked public access, and access restricted to Amazon CloudFront origin access identity.

Additional resources

AWS services

- AWS CloudFormation
- AWS IoT Core
- AWS Lambda
- Amazon DynamoDB
- Amazon Simple Notification Service
- Amazon Simple Storage Service
- Amazon Cognito
- Amazon CloudFront
- AWS AppSync
- AWS Amplify

Related AWS Solutions

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

Appendix A: Solution web interface

The Amazon Virtual Andon 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), and identify the root causes.
  - **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. Use the following procedure to edit an existing site.

1. Sign in to the Amazon Virtual Andon 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)
- 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

Edit the processes for the area

1. On the **Areas** page, identify the area you want to edit and choose **Processes**.
2. On the **Processes** page, identify the process you want to edit and choose **Detail**.
3. On the **Events** page, you can take the following actions:
    - Add a new event by choosing **Add Event**

      > **Note:** In the **Event Registration** dialog box, enter the required information including the **Event Name**, **Event Description**, and the **Event Priority**. Enter the other optional information and choose **Register**.

    - Search for an event using the search tool
    - Delete an event you no longer need to monitor

Users page

For information to set up a new user, refer to Step 3. Use the following procedure to edit the information for an existing user.

1. Sign in to the Amazon Virtual Andon 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. Use the following procedure to delete existing root causes.

1. Sign in to the Amazon Virtual Andon 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.

Use the following procedure to edit permissions for existing users.

1. Sign in to the Amazon Virtual Andon 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 enable or disable 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**.

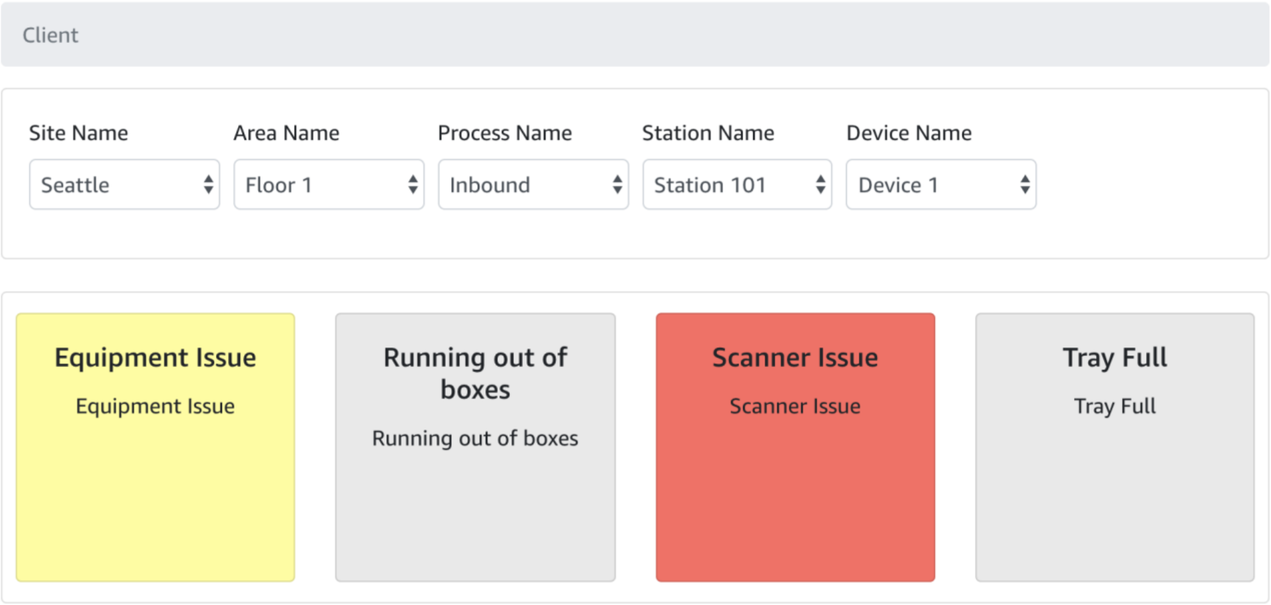
Client page

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 events are displayed as text boxes that represent potential issues that can occur with the selected device. 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 4 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.



Client

Site Name: Seattle
Area Name: Floor 1
Process Name: Inbound
Station Name: Station 101
Device Name: Device 1

Equipment Issue
Equipment Issue

Running out of boxes
Running out of boxes

Scanner Issue
Scanner Issue

Tray Full
Tray Full

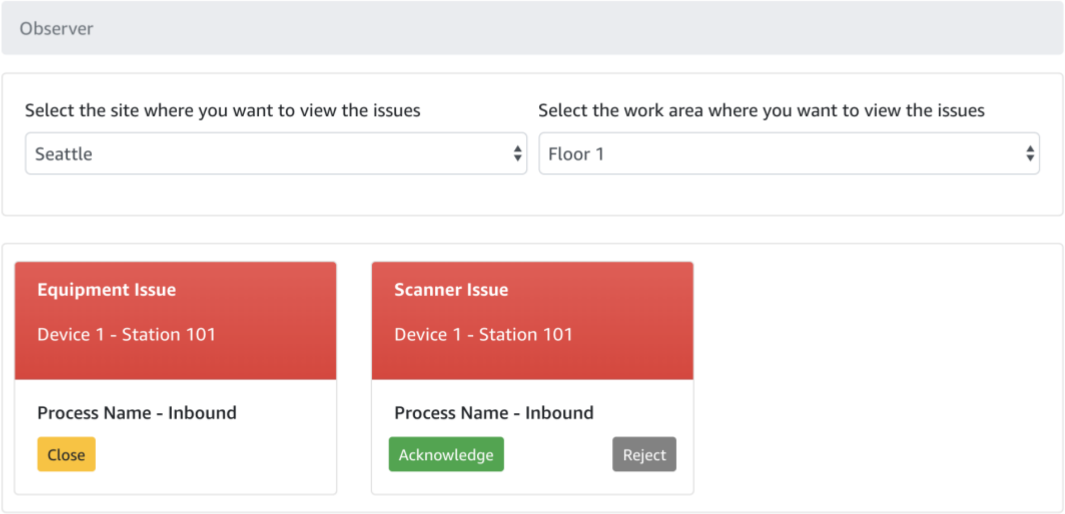
Figure 4: Client console issue status

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 and area. Additionally, they can acknowledge, close, and reject issues.

When engineers close issues, they can choose one of the pre-defined root causes of the event if the event has root causes attached.

Refer to Figure 5 for an example of the Observer page displaying issue statuses.



Observer

Select the site where you want to view the issues: Seattle

Select the work area where you want to view the issues: Floor 1

Equipment Issue
Device 1 - Station 101
Process Name - Inbound

Scanner Issue
Device 1 - Station 101
Process Name - Inbound

Figure 5: Live view showing issue statuses

Analysis page

Users assigned to the Admin and Manager groups can view historical information about issues that have occurred over the last seven days. The analysis page includes the following components.

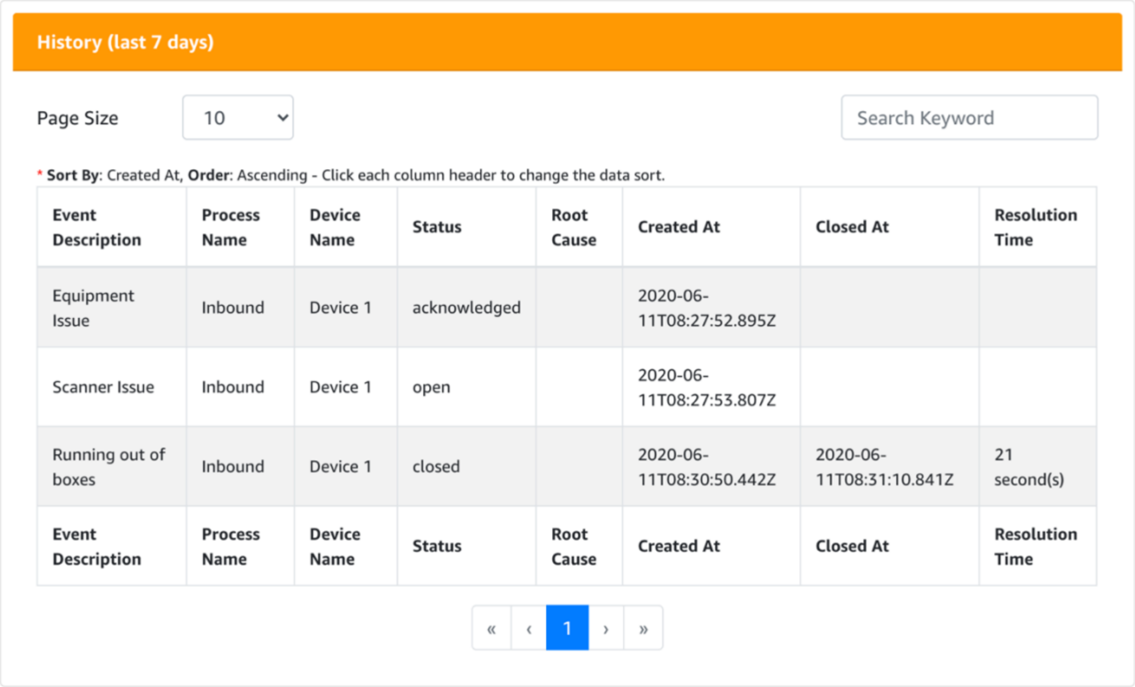
Metrics view

The metrics view enables managers to view metrics of issues that have occurred for the selected sites and areas in the last seven days. The following metrics are available:

- Number of issues per day
- Number of issues over a three hour period of time, covering the last 24 hours
- Total downtime resulting from issues in the last seven days; rejected issues do not have downtime
- Top occurring events grouped by number of occurring issues per event

History view

The history view enables managers to view a complete list of the issues that have occurred in the last seven days for the selected sites and areas. Managers can search, sort, and download the list as a CSV file.



History (last 7 days)

Page Size 10

* **Sort By:** Created At, **Order:** Ascending - Click each column header to change the data sort.

Event Description	Process Name	Device Name	Status	Root Cause	Created At	Closed At	Resolution Time
Equipment Issue	Inbound	Device 1	acknowledged		2020-06-11T08:27:52.895Z		
Scanner Issue	Inbound	Device 1	open		2020-06-11T08:27:53.807Z		
Running out of boxes	Inbound	Device 1	closed		2020-06-11T08:30:50.442Z	2020-06-11T08:31:10.841Z	21 second(s)
Event Description	**Process Name**	**Device Name**	**Status**	**Root Cause**	**Created At**	**Closed At**	**Resolution Time**

Figure 6: History view

Appendix B: 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>0190E0B4E385D7D5</RequestId>
 <HostId>
csOENhmQLVyCEKxVzBuTd0aLaMM0fY8IROZ5rmijF2Tbu3EU85gGPQjrI9VSWnmQAMht
ggKvxmFI=
 </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 view 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 Amazon Virtual Andon 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, the solution 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.

Appendix C: System integration

The Amazon Virtual Andon solution enables 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.

For example, if you are connecting industrial equipment such as OPC DA servers, or Mitsubishi PLC's using the Machine to Cloud Connectivity Framework solution, you can create an IoT rule to trigger an AWS Lambda function that can convert your machine data into the specified format and then publish the message to the `ava/issues` topic.

Appendix D: 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:

```
## 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)
}
```

Appendix E: Migrate from solution version 1 to version 2

This implementation guide contains information about how to set up and configure Amazon Virtual Andon version 2.x and above. You cannot update version 1 of the solution to version 2 using the AWS CloudFormation console due to changes with how resources are deployed. To use version 2, you must launch a new stack using version 2 of the AWS CloudFormation template.

Refer to the following table for a list of the major differences between versions 1 and 2 of this solution.

	Version 1	**Version 2**
Solution deployment	Resources are deployed by AWS CloudFormation template, AWS CodePipeline, and Amplify CLI.	Resources are deployed by AWS CloudFormation template.
Amazon DynamoDB tables	Site table Area table Process table Event table Station table Device table	Site table Area table Process table Event table Station table Device table

	Version 1	Version 2
	Issue table	Issue table Permission table Root cause table
The Users page available on the web interface	No	Yes
The Permissions page to manage the Associate Group available on the web interface	No	Yes
Selection cache at Client page	No	Yes

Users created in version 1 cannot be migrated to version 2. The solution administrator must manually recreate users in version 2. However, the web interface provides a CSV template to upload multiple users at once from the **Users** page. For guidance, refer to Step 3.

> **Note:** User passwords from version 1 cannot be migrated to version 2. Users will receive an email after they have been added in version 2. The email contains the URL to the web interface and the sign-in credentials, including a temporary password that users must change.

Use the following steps to migrate your Amazon DynamoDB tables.

1. Migrate your Amazon DynamoDB table data. Use the following table names:

Table	Version 1	Version 2
Site table	Site-<hash>-<your stack name>	<your stack name>-SiteTable-<hash>
Area table	Area-<hash>-<your stack name>	<your stack name>-AreaTable-<hash>
Process table	Process-<hash>-<your stack name>	<your stack name>-ProcessTable-<hash>
Event table	Event-<hash>-<your stack name>	<your stack name>-EventTable-<hash>
Station table	Station-<hash>-<your stack name>	<your stack name>-StationTable-<hash>
Device table	Device-<hash>-<your stack name>	<your stack name>-DeviceTable-<hash>
Issue table	Issue-<hash>-<your stack name>	<your stack name>-IssueTable-<hash>

The table schema is exactly the same between the two versions. If you have less than 200,000 items in each table, you can use the Amazon Virtual Andon migration template[1]. If you have more data, refer to Exporting and Importing DynamoDB Data Using AWS Data Pipeline in the *Amazon DynamoDB Developer Guide*.

2. Because Amazon DynamoDB table migration does not include Amazon Simple Notification Service (Amazon SNS) topic migration, you must create new Amazon SNS topics, and update the `topicArn` attribute for each item in the `event` Amazon DynamoDB table. You can update topic ARNs by updating events using the solution version 2 web interface.
3. After user and table data migration is finished, the Amazon Virtual Andon web interface displays the exact same data as version 1. After confirming that version 2 of the Amazon Virtual Andon solution has identical data, you can terminate version 1 of the solution.

Appendix F: Uninstall the solution

You can uninstall the Amazon Virtual Andon solution using the AWS Management Console or the AWS Command Line Interface (AWS CLI). However, the Amazon Simple Storage Service (Amazon S3) buckets, Amazon Simple Notification Service (Amazon SNS) topics created for Amazon Virtual Andon events, 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>
```

[1] The AWS CloudFormation template does not support cross Region data migration. It takes approximately four to six minutes to migrate approximately 100,000 items. The template launches an AWS Lambda function, which times out after 15 minutes. When the migration is completed, a notification is sent through Amazon Simple Notification Service (Amazon SNS). You can also view migration result from the AWS CloudFormation console by accessing the Outputs tab.

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**.

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

Alternatively, you can configure the AWS CloudFormation template to delete the Amazon S3 buckets automatically. Prior to deleting the stack, change the deletion behavior in the AWS CloudFormation DeletionPolicy Attribute.

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**.

Deleting the Amazon SNS topics

Use the following AWS CLI command to delete the Amazon SNS topics.

```
for arn in `aws resourcegroupstaggingapi get-resources --tag-filters
Key=amazon-virtual-andon,Values=amazon-virtual-andon --region YOUR_REGION
--query 'ResourceTagMappingList[*].[ResourceARN]' --output text`
do
  aws sns delete-topic --topic-arn $arn --region YOUR_REGION
done
```

Appendix G: 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 enabled, 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
- **Default Language:** The default language selection for the web interface

AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, modify the AWS CloudFormation template mapping section as follows:

```
Send:
  AnonymousUsage:
    Data: "Yes"
```

to

```
Send:
  AnonymousUsage:
    Data: "No"
```

Source code

You can visit our GitHub repository to download the templates and scripts for this solution, and to share your customizations with others.

Document revisions

Date	Change
November 2019	Initial version
July 2020	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
August 2020	Release version 2.1.0: added multi language support; for more information, refer to the CHANGELOG.md file in the GitHub repository

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.