Aspect Workforce™ Integrations for Amazon Connect Configuration Guide

RELEASE DATE: 8/2018

REVISED DATE: 5/10/2026

Legal Notices

The content of this publication is furnished for informational use only and should not be construed as a commitment by Alvaria, Inc. f/k/a Alvaria Software, Inc. (“Alvaria”). Alvaria assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication. Alvaria reserves the right to change information in this publication without notice as a result of product enhancements or other reasons.

Alvaria™, Alvaria®, Unified IP® and other marks as indicated are trademarks or registered trademarks of Alvaria, Inc. in the United States and other countries. Use of any Alvaria trademark is prohibited unless expressly approved in writing in advance by an authorized representative of Alvaria, Inc. Microsoft Windows®, and Microsoft SQL Server® are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Any other brands, product names, company names, logos, trademarks, and/or service marks used in this publication are the property of their respective owners. You may not copy, modify or display any of Alvaria’s or its affiliates’ or licensors’ trademarks, trade names or logos appearing in this publication in any way without Alvaria’s express written consent.

The works of authorship, including but not limited to all design, text and images, contained and the software described in this publication are owned by Alvaria or its affiliates or licensors, except as otherwise expressly stated. The entire contents of this publication are protected by United States and worldwide copyright laws and treaty provisions. In accordance with these laws and provisions, you may not copy, reproduce, modify, use, republish, upload, post, transmit or distribute in any way material from this publication. Further, except as permitted by your written agreement with Alvaria, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, or otherwise, without the prior written permission of Alvaria.

RESTRICTED RIGHTS LEGEND

This publication is provided with “Restricted Rights”. No part of this publication may be photocopied, reproduced or transmitted, in any form or by any means, without the prior written consent of Alvaria. Use, duplication, or disclosure by the United States Government (“Government”) is subject to the restrictions set forth in DFARS 252.227-7013 (b)(3) and FAR 52.227-19. Use of the materials by the Government constitutes acknowledgement of Alvaria’s proprietary rights in them Alvaria is located at 211 Perimeter Center Parkway NE, Suite 250, Atlanta, GA 30346, USA.

LIMITED RIGHTS NOTICE (DEC 2007)

(a) These data are submitted with limited rights under Alvaria’s contracts with various Government entities. These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the Alvaria, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any, provided that the Government makes such disclosure subject to prohibition against further use and disclosure: None.

(b) This notice must be marked on any reproduction of these data, in whole or in-part.

EXPORT

This item is subject to U.S. export control laws and regulations. This item may not be exported, re-exported, re-transferred, disclosed or otherwise diverted contrary to U.S. export control laws or regulations.

NO WARRANTY

THE CONTENTS OF THIS PUBLICATION ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THAT OPERATION OF THE PRODUCTS SOLD BY ALVARIA WILL BE UNINTERRUPTED OR ERROR FREE.

NO LIABILITY

ALVARIA, ITS AFFILIATES, AND LICENSORS ARE NOT LIABLE FOR ANY DAMAGES SUFFERED AS A RESULT OF USING THE CONTENTS OF THIS PUBLICATION. IN NO EVENT WILL ALVARIA, ITS AFFILIATES OR LICENSORS BE LIABLE FOR ANY (i) CONSEQUENTIAL, INDIRECT, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES, (ii) ANY INTERRUPTION OF BUSINESS OR OPERATIONS, COST OF COVER, GOODWILL, TOLL FRAUD, OR LOSS OF DATA, PROFITS, OR REVENUE, OR (iii) FAILURE OF A REMEDY TO ACHIEVE ITS ESSENTIAL PURPOSE. THE LIMITATIONS IN THIS SECTION WILL APPLY TO ANY DAMAGES, HOWEVER CAUSED, AND ON ANY THEORY OF LIABLITY, WHETHER FOR BREACH OF CONTRACT, TORT, MISREPRESENTATION, NEGLIGENCE, THE USE OR PERFORMANCE OF A PRODUCT OR SERVICE, OR OTHERWISE AND REGARDLESS OF WHETHER THE DAMAGES WERE FORESEEABLE OR UNFORSEEABLE. NEITHER PARTY WILL BE LIABLE FOR ANY CLAIM BROUGHT BY THE OTHER PARTY MORE THAN 12 MONTHS AFTER THE OTHER PARTY BECAME AWARE OF THE ISSUE GIVING RISE TO THE CLAIM. ALVARIA’S, ITS AFFILIATES’ OR LICENSORS’ FAILURE TO EXERCISE A RIGHT OR REMEDY IS NOT A WAIVER. BECAUSE SOME JURISDICTIONS PROHIBIT THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

PROGRAMMING AND USE OF PRODUCTS

THE PRODUCTS DESCRIBED IN THIS PUBLICATION CAN BE USED AND PROGRAMMED IN A WIDE VARIETY OF WAYS BASED ON THE REQUIREMENTS OF YOUR PARTICULAR TECHNOLOGY, ENVIRONMENT AND BUSINESS. NOTWITHSTANDING THE USE OF EXAMPLES IN THIS PUBLICATION OR THE PROVISION OF PROFESSIONAL SERVICES BY ALVARIA, ALVARIA RESELLERS, OR ANY THIRD PARTY ENGAGED BY ALVARIA, IT IS IN ALL CASES YOUR RESPONSIBILITY TO ENSURE THAT THE PRODUCTS ARE PROGRAMMED AND USED IN ACCORDANCE WITH ALL APPLICABLE LAWS AND REGULATIONS AND IN A MANNER THAT DOES NOT VIOLATE THE INTELLECTUAL PROPERTY OR OTHER RIGHTS OF ANY THIRD-PARTY.

Rev J
February 4, 2025

Contents

Revision History

Date	Description	Section
August 2018	Rev A, initial publication	NA
November 2020	Rev B, Updates for multiple SQS queues and Agent Hierarchy Group filtering	Architecture, Deployment Steps, Security
December 2020	Rev C, Updates to support KMS encryption	Deployment Steps, Security
May 2021	Rev D, Updates to support the Contact Data by Routing Profile report in WFM Adapter security changes for RTA	Overview, Deployment Steps, Security
February 2023	Rev E, Updates and corrections related to the AWS Console interface	Overview, Architecture, Prerequisites, Deployment Options, Deployment Steps, Security, FAQ
August 2023	Rev F, Updates to Agent Productivity logic. Branding updates.	Overview, Architecture, Deployment Options, Deployment Steps, Security
November 2023	Rev G, update to link to AWS Data Streaming document	Deployment Steps
April 2024	Rev H, Updates to support using IAM roles in WFM Adapter and RTA	Architecture, Deployment Steps, Security
August 2024	Rev I, updates related to hosting assets in aspect-workforce S3 bucket. Remove references to the AWS QuickStart program. Branding updates.	Overview, Architecture, Deployment Options, Deployment Steps, Security
February 2025	Rev J, updates to clarify the use of Amazon's Cloud Formation Stack to quickly create the necessary objects in Amazon Web Services for either Agent Productivity, Real-Time Adherence, or both. Clarification that a single Aspect WFM Adapter can be configured to pull historical data from multiple Amazon Connect instances.	Architecture, Agent Productivity

May 2026	Rev K, updates to support the Amazon Connect (API) data source type in WFM Adapter.	Architecture, Deployment Options, Best Practices Using Aspect Workforce™ on AWS, Security

Overview

This Configuration guide provides step-by-step instructions for deploying Aspect Workforce™ integrations with Amazon Connect in the Amazon Web Services (AWS) Cloud.

These integrations are for users of Aspect Workforce™ who want to supply Amazon Connect historical agent productivity and/or real-time adherence data into their Workforce system.

Aspect Workforce™ (WFM) on AWS

The following integration options are supported:

- Agent productivity – Enhances the standard Amazon Connect reports with statistics based on agent sign-in/sign-out information. You can designate whether custom agent status labels defined in Amazon Connect should be treated as available, signed in, or signed out. For example, a custom agent status called “Break,” which represents the agent taking time off from work, would typically be treated as signed out, whereas a custom agent status called “Project,” which represents some sort of project work, would typically be treated as signed in. Aspect Workforce™ uses this information to produce statistics on average positions staffed (APS) by agent group, available time by agent, unavailable time by agent, and sign-in/sign-out pairs by agent.
- Real-time adherence – Provides Amazon Connect agent state change information to the Aspect Real-Time Adherence (RTA) product, which enables you to monitor the activities of your Amazon Connect agents and monitor how well these activities adhere to the agents’ schedules.

Both integration options use an Amazon Connect agent event stream. An Amazon Connect instance supports a single agent event stream. If you have already enabled agent event streams and selected a Kinesis stream for that purpose, choose one of the deployment options that uses an existing Kinesis data stream. If agent event data streaming is not currently enabled for your Amazon Connect instance, choose a deployment option that creates a new Kinesis data stream.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this deployment. There is no additional cost for using the integration. These integrations require Aspect Workforce™ version 18.2 or higher and Aspect WFM Adapter version 3.3 or higher.

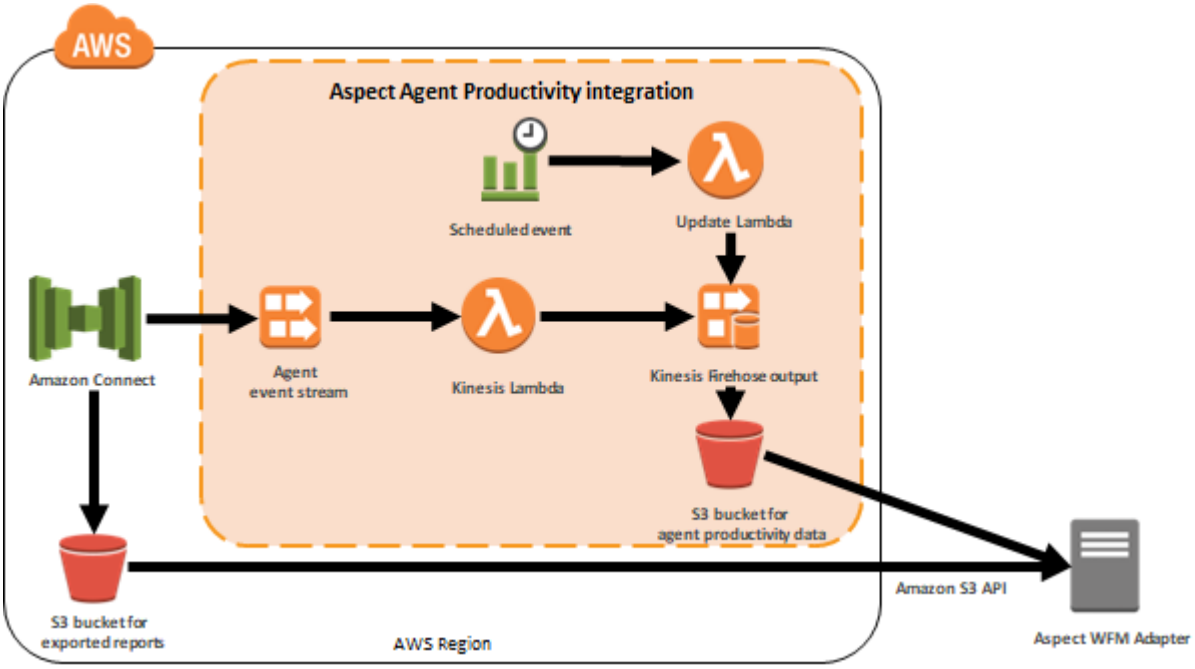
For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Architecture

Aspect uses Amazon's Cloud Formation Stack to quickly create the necessary objects in Amazon Web Services for either Agent Productivity, Real-Time Adherence, or both.

Agent Productivity

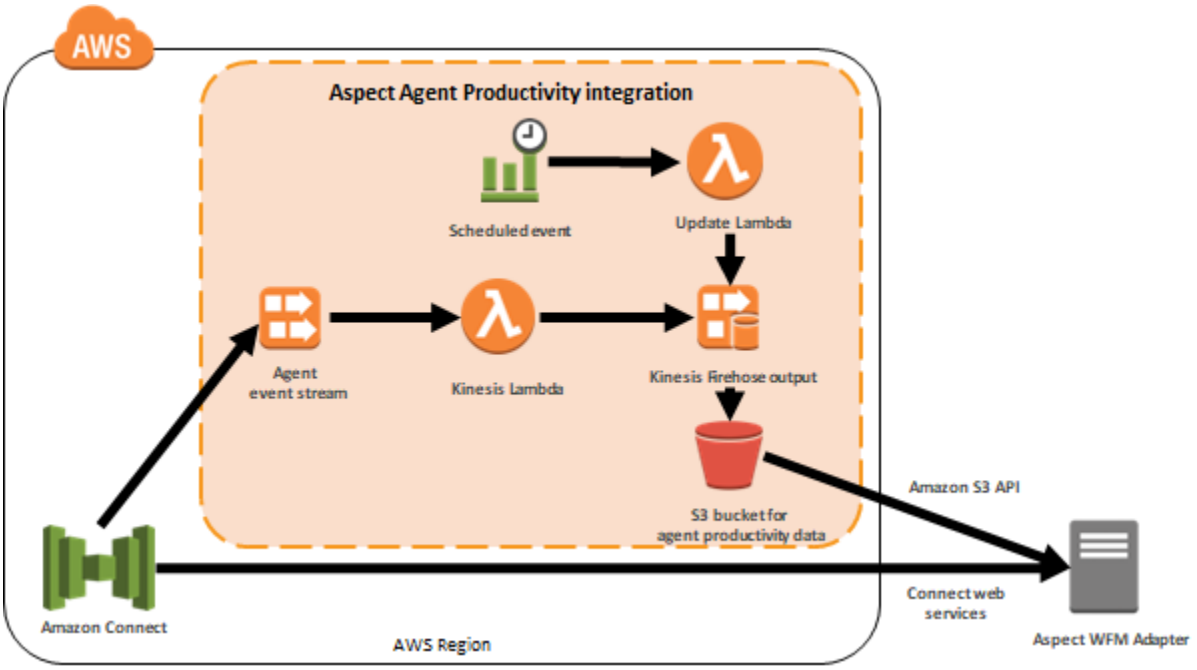
Deploying Aspect's Quick Create Cloud Formation Stack integration that includes **Agent Productivity** builds one of the following environments in the AWS Cloud.



This integration is used with the Amazon Connect data source type in WFM Adapter. It sets up the following:

- An S3 bucket that holds the Agent Productivity outputs.
- A Kinesis Lambda function that reads agent events from your Amazon Connect instance. The Lambda function categorizes those agent events as spans of signed-in or signed-out time.
- A Kinesis Data Firehose data delivery stream that writes the output of the Kinesis Lambda function to the S3 bucket.
- An update Lambda function that also writes to the Kinesis Data Firehose data delivery stream. The update Lambda function ensures that output objects are written to the S3 bucket during periods of time when no agents are signed-in.
- A CloudWatch Events rule that calls the update Lambda function on a schedule, every five minutes.
- An IAM user or IAM role to provide read access to objects in the two S3 buckets used by WFM Adapter:

- The S3 bucket for exported reports, associated with your Amazon Connect instance. You will need to schedule the export of several Amazon Connect reports. For details, see the Aspect WFM Adapter documentation.
- The S3 bucket created by this integration.



This integration is used with the Amazon Connect (API) data source in WFM Adapter. It sets up the following:

- An S3 bucket that holds the Agent Productivity outputs.
- A Kinesis Lambda function that reads agent events from your Amazon Connect instance. The Lambda function categorizes those agent events as spans of signed-in or signed-out time.
- A Kinesis Data Firehose data delivery stream that writes the output of the Kinesis Lambda function to the S3 bucket.
- An update Lambda function that also writes to the Kinesis Data Firehose data delivery stream. The update Lambda function ensures that output objects are written to the S3 bucket during periods of time when no agents are signed-in.
- A CloudWatch Events rule that calls the update Lambda function on a schedule, every five minutes.
- An IAM user or IAM role to provide the required access to WFM Adapter:
- Read-only access to the S3 bucket created by this integration.
- Access to call the following Connect web services: DescribeUserHierarchyGroup, GetMetricDataV2, ListQueues, ListRoutingProfiles, ListUsers, and SearchUserHierarchyGroups.

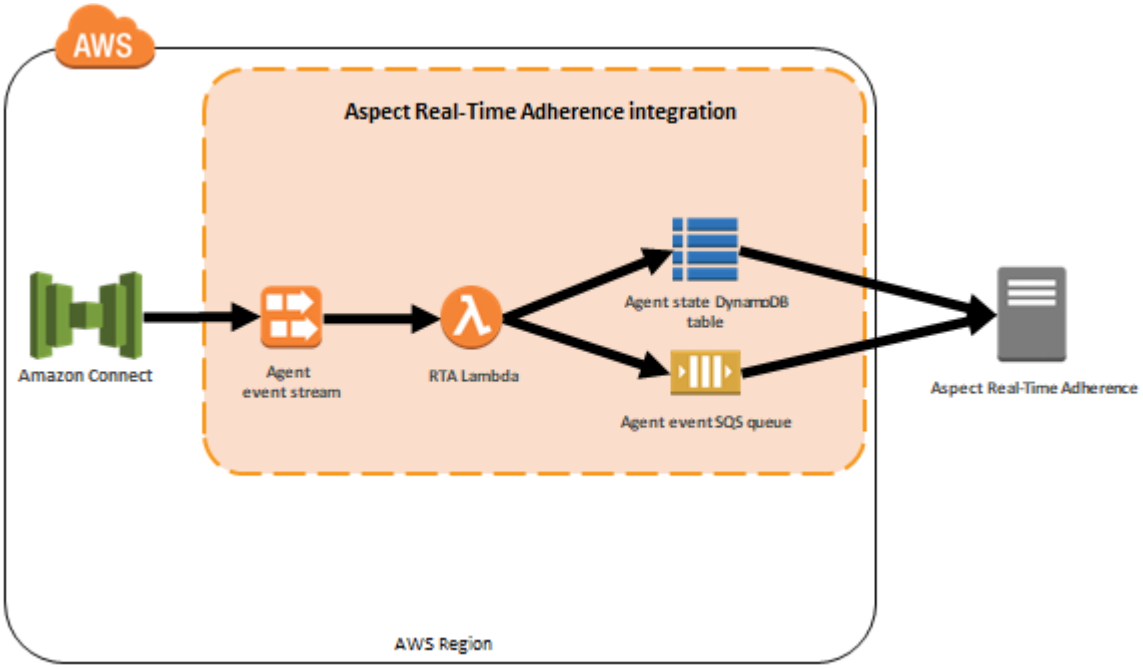
You will need to deploy a separate Quick Create Cloud Formation Stack integration for each Amazon Connect instance for which Agent Productivity support is required.

A single Aspect WFM Adapter can be configured to pull historical data from multiple Amazon Connect instances.

Note: the Amazon Connect (API) data source type is available starting in WFM Adapter version 21.0.255.0. Aspect recommends using the Amazon Connect (API) data source type. Contact Aspect Support for more information about upgrading WFM Adapter.

Real-Time Adherence

Deploying Aspect's Quick Create Cloud Formation Stack integration that includes **Real-Time Adherence** builds the following environment in the AWS Cloud.



The integration sets up the following:

- A DynamoDB table that holds the latest state change for each agent signed into your Amazon Connect instance.
- An optional DynamoDB table that holds configuration information. If you choose to store RTA configuration in a table, the integration will create this table. If you choose to store RTA configuration in the environment variables of the RTA Lambda, the integration will not create this table.
- One or more SQS queues that are used to relay Amazon Connect agent state changes to the Aspect Real-Time Adherence product. By default, the integration will create a single SQS queue. You can create multiple SQS queues (up to 10) to improve the throughput of state changes.
- A Lambda function that is called whenever your Amazon Connect instance writes events to its agent event Kinesis data stream. The Lambda function is responsible for updating the DynamoDB table and SQS queue(s) created by the integration.
- In cases where an RTA server is configured to monitor a subset of the agents associated with an Amazon Connect instance, you should configure the integration to filter based on Agent Hierarchy Groups. To do so, identify an Agent Hierarchy Group Level configured in the Amazon Connect instance that can be used to distinguish the agents being monitored on the RTA server. Configure AHGFilterLevel to match the Agent Hierarchy Group Level number (1-5). Configure a list of Agent Hierarchy Group names that are available for the specified level and match the agents to be included. By default, group names should be separated by commas. However, you can specify a different separator in AHGFilterSeparator if some of your group names contain commas.

  Note: if you want to send all state changes to the RTA server, use the default AHGFilterLevel value of 0.

- An IAM user or IAM role to provide access to the AWS resources required by Aspect Real-Time Adherence:
  - Read-only access to the DynamoDB table that holds the latest state change for each agent signed into your Amazon Connect instance.
  - Read/write access to the SQS queue(s).
  - If configuration information is stored in a table:
    - Read/write access to the configuration DynamoDB table.
  - Otherwise,
    - Access to read and update the configuration of the Lambda function.

You will need to deploy a separate Quick Create Cloud Formation Stack integration for each Amazon Connect instance connection to an Aspect Real-Time Adherence server. That is, if you wish to monitor agent states from an Amazon Connect instance on two different Aspect Real-Time Adherence servers, then you will need to deploy a separate Quick Create Cloud Formation Stack integration for each RTA server.

If you choose to add Aspect Workforce with a new Kinesis data stream, the following resources will be created:

- A Kinesis data stream to be configured as the agent event stream of your Amazon Connect instance. This Kinesis data stream is designated as “Agent event stream” in the figures above.

Prerequisites

Specialized Knowledge

Before you deploy this integration, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.)

- Amazon Connect
- Amazon S3
- Amazon DynamoDB
- Amazon SQS
- Amazon Kinesis
- AWS Lambda
- Amazon CloudWatch
- AWS CloudFormation

Deployment Options

This integration provides six deployment options divided into two categories:

- ***Add Aspect Workforce™ with a new Kinesis data stream***. Choose this category if agent event data streaming is not currently enabled for your Amazon Connect instance. This category includes three deployment options:
  - ***Deploy for agent productivity*.** Choose this option if you plan to use the Agent Productivity feature of Aspect Workforce but not the Real-Time Adherence feature of Aspect Workforce.
  - ***Deploy for real-time adherence.*** Choose this option if you plan to use the Real-Time Adherence feature of Aspect Workforce but not the Agent Productivity feature of Aspect Workforce.
  - ***Deploy for both options.*** Choose this option if you plan to use both the Agent Productivity and Real-Time Adherence features of Aspect Workforce.
- ***Add Aspect Workforce™ with an existing Kinesis data stream***. Choose this category if agent event data streaming is enabled for your Amazon Connect instance, and you have selected a Kinesis stream for that purpose. This category includes three deployment options:
  - ***Deploy f*or ***agent productivity***. Choose this option if you plan to use the Agent Productivity feature of Aspect Workforce but not the Real-Time Adherence feature of Aspect Workforce. You can choose this option to add support for the Agent Productivity feature of Aspect Workforce, if you previously deployed support for Real-Time Adherence.
  - ***Deploy for real-time adherence.*** Choose this option if you plan to use the Real-Time Adherence feature of Aspect Workforce but not the Agent Productivity feature of Aspect Workforce. You can choose this option to add support for the Real-Time Adherence feature of Aspect Workforce, if you previously deployed support for Agent Productivity. You will need to choose this option if you want to monitor your Amazon Connect instance from multiple Aspect Real-Time Adherence servers. You will need to deploy this option once for each additional Real-Time Adherence server.
  - ***Deploy for both options.*** Choose this option if you plan to use both the Agent Productivity and Real-Time Adherence features of Aspect Workforce.

The integration provides templates for these options. It also lets you configure Aspect Workforce™ settings, as discussed later in this guide.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Aspect Workforce™ on AWS. You must select the same AWS Region as your Amazon Connect instance.

Step 2. Check Your Amazon Connect Instance

1. Edit your Amazon Connect instance within the AWS console.
2. Select Data streaming. Verify whether the Enable data streaming checkbox is checked and a Kinesis Stream is selected under Agent Events.

    a. If Agent Event data streaming is enabled for your Amazon Connect instance, you should choose one of the deployment options listed under the category "Add Aspect Workforce with an existing Kinesis data stream," in the next step.

    b. If Agent Event data streaming is NOT enabled, you should choose one of the deployment options listed under the category "Add Aspect Workforce with a new Kinesis data stream," in the next step.

3. If Agent Event data streaming is enabled for your Amazon Connect instance, switch to the Amazon Kinesis service, edit the Kinesis data stream that was selected as the Agent Event stream, and locate the Stream ARN. We recommend that you copy the Stream ARN to the clipboard, so you can paste it as the value of the Agent Event Kinesis Stream ARN in the next step.

Step 3. Launch the Integration

Note: You are responsible for the cost of the AWS services used while running this integration. There is no additional cost for using this integration. For full details, see the pricing pages for each AWS service you will be using in this integration. Prices are subject to change.

When you are ready to create a deployment for the Aspect Workforce™ Integration with AWS:

1. Go here. This page will review the Deployment Options discussed earlier.
2. Click on the appropriate deployment link in the **Deployment options** section. This will open a new page with the corresponding template already selected and several options.
3. Change the **Stack name** if needed.

4. For all other parameters, review the default settings and customize them as necessary. Links to the parameters for each deployment option are listed below.
5. When you finish, review the information in the blue box at the bottom and check all checkboxes.
6. Click **Create Stack** to deploy the stack.
    c. Clicking **Create change set** will provide you with several advanced options not covered in this guide. Contact Amazon for more information.
7. Monitor the status of the stack.
8. When the target stack status is **CREATE_COMPLETE**, the Aspect Workforce™ integration is ready.
9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

In the following tables, parameters are listed by category and described separately for the six deployment options:

- Parameters for deploying Aspect Agent Productivity with a new Kinesis data stream
- Parameters for deploying Aspect Real-Time Adherence with a new Kinesis data stream
- Parameters for deploying Aspect Agent Productivity and Real-Time Adherence with a new Kinesis data stream
- Parameters for deploying Aspect Agent Productivity with an existing Kinesis data stream
- Parameters for deploying Aspect Real-Time Adherence with an existing Kinesis data stream
- Parameters for deploying Aspect Agent Productivity and Real-Time Adherence with an existing Kinesis data stream

Option 1: Deploying Aspect Agent Productivity with a New Kinesis Data Stream

View template

Aspect Workforce™ Configuration:

Parameter label (name)	Default	Description
Kinesis Firehose Stream Name (FirehoseStreamName)	aspect-wfm-ap-kda-to-s3	Enter the name of the Kinesis Firehose stream to create. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). If you have multiple Amazon Connect instances in your AWS account, you will need to create a Kinesis Firehose stream for each Amazon Connect instance and give each stream a unique name. The name of the Kinesis Firehose stream determines the filenames of agent productivity report files written to S3. By default, WFM Adapter expects the report files to be named based on a Kinesis Firehose stream name of “aspect-wfm-ap-kda-

Parameter label (name)	Default	Description
		to-s3". If you specify a different stream name, be sure to update the WFM Adapter configuration for the corresponding data source to match your stream name, in the Firehose Report Mapping data source parameter. Consult the WFM Adapter help for more information.
Agent Productivity Report Prefix (ApDataS3Prefix)	OUTPUT/	Enter the prefix for Agent Productivity reports written to S3. You should configure the corresponding WFM Adapter data source to match this value, in the Firehose Report Root Path data source parameter.
Agent Status Name Separator (StatusSeparator)	,	Character used to separate signed-out agent status names. You should configure a separator character that does not appear in any of the individual names
Signed-Out Agent Status Names (SignedOutStatuses)		Enter the list of agent status names for agent statuses that should be treated as signed-out in WFM. For example, an agent status named Break which agents use during a scheduled break would typically be listed here. Multiple signed-out agent status names may be listed. Names should be separated by the configured Agent Status Name Separator. The agent status with a Type of OFFLINE, by default named Offline, will always be treated as signed-out.

Amazon Connect Configuration:

Parameter label (name)	Default	Description
Amazon Connect Metric Source	S3	Select S3 if WFM Adapter should calculate statistics by querying Exported S3 reports. Select API if WFM Adapter should calculate statistics by calling Connect web services. If you select S3, you should create an Amazon Connect data source in the WFM Adapter UI. If you select API, you should create an Amazon Connect (API) data source in the WFM Adapter UI.

Parameter label (name)	Default	Description
Amazon Connect Exported Reports Bucket (ConnectS3Bucket)		Enter the name of the Exported reports S3 bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Prefix (ConnectS3Prefix)	connect/directory/Reports/Aspect/	Enter the prefix under which the exported reports read by WFM Adapter will be exported, in the Exported reports bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Bucket KMS Key ARN (ConnectS3KmsArn)		(Optional) Amazon Resource Name (ARN) of the KMS key required to decrypt the exported reports of your Amazon Connect instance. You should supply this ARN if you configured your exported reports bucket to use server-side encryption with a customer-managed customer master key (CMK). Otherwise, you should leave this parameter blank.
Amazon Connect Instance ARN		Amazon Resource Name (ARN) of the Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is API.

IAM Configuration

Parameter label (name)	Default	Description
Authorization Mode (AuthorizationMode)	User	Select User to create an IAM User for WFM Adapter. Select Role to create an IAM Role for WFM Adapter. If WFM Adapter is running outside of AWS, you should select User. If WFM Adapter is running inside AWS, you should select Role.
Source AWS Account ID (SourceAwsAccountId)		Optional AWS account ID to include in the trust policy for the IAM Role. The AWS account ID should match the AWS account from which WFM Adapter will assume the role. This parameter is required when Authorization Mode is Role. This parameter will be ignored when Authorization Mode is User.
External ID (ExternalId)		Optional external ID to include in the trust policy for the IAM Role. If Authorization Mode is Role, the role

Parameter label (name)	Default	Description
		will be configured to require this external ID. You will need to configure WFM Adapter to supply this external ID when it assumes the role. If Authorization Mode is User, this parameter will be ignored.

Deployment Configuration

Parameter label (name)	Default	Description
Deployment S3 Bucket Name (DeploymentS3BucketName)	aspect-workforce	S3 bucket for the deployment assets, An S3 bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Deployment S3 Key Prefix (DeploymentS3KeyPrefix)	aspect-workforce-connect-integration/	S3 key prefix for the deployment assets. Deployment key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Option 2: Deploying Aspect Real-Time Adherence with a New Kinesis Data Stream

View template

Aspect Workforce™ Configuration:

Parameter label (name)	Default	Description
Number of SQS Queues (NumSQSQueues)	1	The number of SQS queues to create (must be between 1 and 10). Creating additional SQS queues can reduce the latency of state changes.
Write to SQS Flag Location (LambdaConfigLocation)	env	Once RTA reads an initial set of states from the agent event DynamoDB table, it toggles a Write to SQS flag to ensure that agent events are written to the SQS queue(s). This setting controls where that Write to SQS flag is stored either in an environment variable of the RTA Lambda (**env**) or in a configuration DynamoDB table (**tab**). Storing this flag in an environment variable of the Lambda requires less overhead but requires greater permissions for the RTA user. Storing this flag in a configuration DynamoDB

Parameter label (name)	Default	Description
		table requires fewer permissions for the RTA user but requires an additional DyanmoDB read each time the RTA Lambda executes. By default, this flag will be stored in an environment variable of the RTA Lambda.

Amazon Connect Configuration

Parameter label (name)	Default	Description
Agent Hierarchy Group Level (AHGFilterLevel)	0	The Agent Hierarchy Group Level on which agent events should be filtered (must be between 0 and 5). Configuring a value of 0 disables filtering. Configuring a value between 1 and 5 means that agent events will be filtered based on that Agent Hierarchy Group Level.
Agent Hierarchy Group filter value separator (AHGFilterSeparator)	,	Character used to separate matching values listed in AHGFilterValues. You should configure a separator character that does not appear in any of the individual matching values.
Agent Hierarchy Group filter matching values (AHGFilterValues)		An optional list of matching Agent Hierarchy Group Level values. If you enable Agent Hierarchy Group filtering, any agent events with an Agent Hierarchy Group Level value matching one of the values listed here will be sent on to Real-Time Adherence and any agent events that do not match the filter will be discarded. Matching values should be separated with the character configured in AHGFilterSeparator.

IAM Configuration

Parameter label (name)	Default	Description
Authorization Mode (AuthorizationMode)	User	Select User to create an IAM User for RTA. Select Role to create an IAM Role for RTA. If RTA is running outside of AWS, you should select User. If RTA is running inside AWS, you should select Role.
Source AWS Account ID (SourceAwsAccountId)		Optional AWS account ID to include in the trust policy for the IAM Role. The AWS account ID should match the AWS account from which RTA will

Parameter label (name)	Default	Description
		assume the role. This parameter is required when Authorization Mode is Role. This parameter will be ignored when Authorization Mode is User.
External ID (ExternalId)		Optional external ID to include in the trust policy for the IAM Role. If Authorization Mode is Role, the role will be configured to require this external ID. You will need to configure RTA to supply this external ID when it assumes the role. If Authorization Mode is User, this parameter will be ignored.

Deployment Configuration

Parameter label (name)	Default	Description
Deployment S3 Bucket Name (DeploymentS3BucketName)	aspect-workforce	S3 bucket for the deployment assets, An S3 bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Deployment S3 Key Prefix (DeploymentS3KeyPrefix)	connect-integration-aspect-wfm/	S3 key prefix for the deployment assets. Deployment key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Option 3: Deploying Aspect Agent Productivity and Real-Time Adherence with a New Kinesis Data Stream

View template

Aspect Workforce™ Configuration

Parameter label (name)	Default	Description
Kinesis Firehose Stream Name (FirehoseStreamName)	aspect-wfm-ap-kda-to-s3	Enter the name of the Kinesis Firehose stream to create. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). If you have multiple Amazon Connect instances in your AWS account, you will need to create a Kinesis Firehose stream for each Amazon Connect instance and give each stream a unique name. The name of the Kinesis

Parameter label (name)	Default	Description
		Firehose stream determines the filenames of agent productivity report files written to S3. By default, WFM Adapter expects the report files to be named based on a Kinesis Firehose stream name of "aspect-wfm-ap-kda-to-s3". If you specify a different stream name, be sure to update the WFM Adapter configuration for the corresponding data source to match your stream name, in the Firehose Report Mapping data source parameter. Consult the WFM Adapter help for more information.
Agent Productivity Report Prefix (ApDataS3Prefix)	OUTPUT/	Enter the prefix for Agent Productivity reports written to S3. You should configure the corresponding WFM Adapter data source to match this value, in the Firehose Report Root Path data source parameter.
Agent Status Name Separator (StatusSeparator)	,	Character used to separate signed-out agent status names. You should configure a separator character that does not appear in any of the individual names
Signed-Out Agent Status Names (SignedOutStatuses)		Enter the list of agent status names for agent statuses that should be treated as signed-out in WFM. For example, an agent status named Break which agents use during a scheduled break would typically be listed here. Multiple signed-out agent status names may be listed. Names should be separated by the configured Agent Status Name Separator. The agent status with a Type of OFFLINE, by default named Offline, will always be treated as signed-out.
Number of SQS Queues (NumSQSQueues)	1	The number of SQS queues to create (must be between 1 and 10). Creating additional SQS queues can reduce the latency of state changes.
Write to SQS Flag Location (LambdaConfigLocation)	env	Once RTA reads an initial set of states from the agent event DynamoDB table, it toggles a Write to SQS flag to ensure that agent events are written to the SQS queue(s). This setting controls where that Write to SQS flag is stored either in an environment variable of the RTA Lambda (**env**) or in a configuration DynamoDB table (**tab**). Storing this flag in an environment

Parameter label (name)	Default	Description
		variable of the Lambda requires less overhead but requires greater permissions for the RTA user. Storing this flag in a configuration DynamoDB table requires fewer permissions for the RTA user but requires an additional DyanmoDB read each time the RTA Lambda executes. By default, this flag will be stored in an environment variable of the RTA Lambda.

Amazon Connect Configuration

Parameter label (name)	Default	Description
Amazon Connect Metric Source	S3	Select S3 if WFM Adapter should calculate statistics by querying Exported S3 reports. Select API if WFM Adapter should calculate statistics by calling Connect web services. If you select S3, you should create an Amazon Connect data source in the WFM Adapter UI. If you select API, you should create an Amazon Connect (API) data source in the WFM Adapter UI.
Amazon Connect Exported Reports Bucket (ConnectS3Bucket)		Enter the name of the Exported reports S3 bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Prefix (ConnectS3Prefix)	connect/directory/Reports/Aspect/	Optional Amazon Resource Name (ARN) of the KMS key required to decrypt the exported reports of your Amazon Connect instance. You should supply this ARN if you configured your exported reports bucket to use server-side encryption with an AWS Key Management Service (KMS) key. Otherwise, you should leave this parameter blank.
Amazon Connect Exported Reports Bucket KMS Key ARN (ConnectS3KmsArn)		(Optional) Amazon Resource Name (ARN) of the KMS key required to decrypt the exported reports of your Amazon Connect instance. You should supply this ARN if you configured your exported reports bucket to use server-side encryption with a customer-managed customer master key (CMK). Otherwise, you should leave this parameter blank.

Parameter label (name)	Default	Description
Amazon Connect Instance ARN		Amazon Resource Name (ARN) of the Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is API.
Agent Hierarchy Group Level (AHGFilterLevel)	0	The Agent Hierarchy Group Level on which agent events should be filtered (must be between 0 and 5). Configuring a value of 0 disables filtering. Configuring a value between 1 and 5 means that agent events will be filtered based on that Agent Hierarchy Group Level.
Agent Hierarchy Group filter value separator (AHGFilterSeparator)	,	Character used to separate matching values listed in AHGFilterValues. You should configure a separator character that does not appear in any of the individual matching values.
Agent Hierarchy Group filter matching values (AHGFilterValues)		An optional list of matching Agent HierarchyGroup Level values. If you enable Agent Hierarchy Group filtering, any agent events with an Agent Hierarchy Group Level value matching one of the values listed here will be sent on to Real-Time Adherence and any agent events that do not match the filter will be discarded. Matching values should be separated with the character configured in AHGFilterSeparator.

IAM Configuration

Parameter label (name)	Default	Description
Authorization Mode (AuthorizationMode)	User	Select User to create IAM Users for WFM Adapter and RTA. Select Role to create IAM Roles for WFM Adapter and RTA. If WFM Adapter and RTA are running outside of AWS, you should select User. If WFM Adapter and RTA are running inside AWS, you should select Role.
Source AWS Account ID (SourceAwsAccountId)		Optional AWS account ID to include in the trust policy for the IAM Role. The AWS account ID should match the AWS account from which WFM Adapter and RTA will assume their roles. This parameter is required when Authorization Mode is Role. This

Parameter label (name)	Default	Description
		parameter will be ignored when Authorization Mode is User.
External ID (ExternalId)		Optional external ID to include in the trust policy for the IAM Role. If Authorization Mode is Role, the role will be configured to require this external ID. You will need to configure WFM Adapter and RTA to supply this external ID when they assume their roles. If Authorization Mode is User, this parameter will be ignored.

Deployment Configuration

Parameter label (name)	Default	Description
Deployment S3 Bucket Name (DeploymentS3BucketName)	aspect-workforce	S3 bucket for the deployment assets, An S3 bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Deployment S3 Key Prefix (DeploymentS3KeyPrefix)	aspect-workforce-connect-integration/	S3 key prefix for the deployment assets. Deployment key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Option 4: Deploying Aspect Agent Productivity with an Existing Kinesis Data Stream

View template

Aspect Workforce™ Configuration

Parameter label (name)	Default	Description
Kinesis Firehose Stream Name (FirehoseStreamName)	aspect-wfm-ap-kda-to-s3	Enter the name of the Kinesis Firehose stream to create. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). If you have multiple Amazon Connect instances in your AWS account, you will need to create a Kinesis Firehose stream for each Amazon Connect instance and give each stream a unique name. The name of the Kinesis Firehose stream determines the filenames of agent productivity report

Parameter label (name)	Default	Description
		files written to S3. By default, WFM Adapter expects the report files to be named based on a Kinesis Firehose stream name of "aspect-wfm-ap-kda-to-s3". If you specify a different stream name, be sure to update the WFM Adapter configuration for the corresponding data source to match your stream name, in the Firehose Report Mapping data source parameter. Consult the WFM Adapter help for more information.
Agent Productivity Report Prefix (ApDataS3Prefix)	OUTPUT/	Enter the prefix for Agent Productivity reports written to S3. You should configure the corresponding WFM Adapter data source to match this value, in the Firehose Report Root Path data source parameter.
Agent Status Name Separator (StatusSeparator)	,	Character used to separate signed-out agent status names. You should configure a separator character that does not appear in any of the individual names
Signed-Out Agent Status Names (SignedOutStatuses)		Enter the list of agent status names for agent statuses that should be treated as signed-out in WFM. For example, an agent status named Break which agents use during a scheduled break would typically be listed here. Multiple signed-out agent status names may be listed. Names should be separated by the configured Agent Status Name Separator. The agent status with a Type of OFFLINE, by default named Offline, will always be treated as signed-out.

Amazon Connect Configuration

Parameter label (name)	Default	Description
Amazon Connect Metric Source	S3	Select S3 if WFM Adapter should calculate statistics by querying Exported S3 reports. Select API if WFM Adapter should calculate statistics by calling Connect web services. If you select S3, you should create an Amazon Connect data source in the WFM Adapter UI. If you select API, you should create an

Parameter label (name)	Default	Description
		Amazon Connect (API) data source in the WFM Adapter UI.
Amazon Connect Exported Reports Bucket (ConnectS3Bucket)		Enter the name of the Exported reports S3 bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Prefix (ConnectS3Prefix)	connect/directory/Reports/Aspect/	Enter the prefix under which the exported reports read by WFM Adapter will be exported, in the Exported reports bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Bucket KMS Key ARN (ConnectS3KmsArn)		Amazon Resource Name (ARN) of the KMS key required to decrypt the exported reports of your Amazon Connect instance. You should supply this ARN if you configured your exported reports bucket to use server-side encryption with a customer-managed customer master key (CMK). Otherwise, you should leave this parameter blank.
Amazon Connect Instance ARN		Amazon Resource Name (ARN) of the Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is API.
Agent Event Kinesis Stream ARN (AgentEventStreamArn)		Enter the Amazon Resource Name (ARN) of the Amazon Kinesis Data Stream to which Amazon Connect delivers Agent Events.
Agent Event Kinesis Stream KMS Key ARN (AgentEventStreamKmsArn)		(Optional) Amazon Resource Name (ARN) of the KMS key required to decrypt agent events. You should supply this ARN if you configured your Agent Event Kinesis stream to use server-side encryption with a customer-managed customer master key (CMK). Otherwise, you should leave this parameter blank.

IAM Configuration

Parameter label (name)	Default	Description
Authorization Mode (AuthorizationMode)	User	Select User to create an IAM User for WFM Adapter. Select Role to create an

Parameter label (name)	Default	Description
		IAM Role for WFM Adapter. If WFM Adapter is running outside of AWS, you should select User. If WFM Adapter is running inside AWS, you should select Role.
Source AWS Account ID (SourceAwsAccountId)		Optional AWS account ID to include in the trust policy for the IAM Role. The AWS account ID should match the AWS account from which WFM Adapter will assume the role. This parameter is required when Authorization Mode is Role. This parameter will be ignored when Authorization Mode is User.
External ID (ExternalId)		Optional external ID to include in the trust policy for the IAM Role. If Authorization Mode is Role, the role will be configured to require this external ID. You will need to configure WFM Adapter to supply this external ID when it assumes the role. If Authorization Mode is User, this parameter will be ignored.

Deployment Configuration

Parameter label (name)	Default	Description
Deployment S3 Bucket Name (DeploymentS3BucketName)	aspect-workforce	S3 bucket for the deployment assets, An S3 bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Deployment S3 Key Prefix (DeploymentS3KeyPrefix)	aspect-workforce-connect-integration/	S3 key prefix for the deployment assets. Deployment key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Option 5: Deploying Aspect Real-Time Adherence with an Existing Kinesis Data Stream

View template

Aspect Workforce™ Configuration

Parameter label (name)	Default	Description
Number of SQS Queues (NumSQSQueues)	1	The number of SQS queues to create (must be between 1 and 10). Creating additional SQS queues can reduce the latency of state changes.
Write to SQS Flag Location (LambdaConfigLocation)	env	Once RTA reads an initial set of states from the agent event DynamoDB table, it toggles a Write to SQS flag to ensure that agent events are written to the SQS queue(s). This setting controls where that Write to SQS flag is stored either in an environment variable of the RTA Lambda (env) or in a configuration DynamoDB table (tab). Storing this flag in an environment variable of the Lambda requires less overhead but requires greater permissions for the RTA user. Storing this flag in a configuration DynamoDB table requires fewer permissions for the RTA user but requires an additional DyanmoDB read each time the RTA Lambda executes. By default, this flag will be stored in an environment variable of the RTA Lambda.

Amazon Connect Configuration

Parameter label (name)	Default	Description
Agent Event Kinesis Stream ARN (AgentEventStreamArn)	(requires input)	Enter the Amazon Resource Name (ARN) of the Amazon Kinesis Data Stream to which Amazon Connect delivers Agent Events.
Agent Event Kinesis Stream KMS Key ARN (AgentEventStreamKmsArn)		(Optional) Amazon Resource Name (ARN) of the KMS key required to decrypt agent events. You should supply this ARN if you configured your Agent Event Kinesis stream to use server-side encryption with a customer-managed customer master key (CMK). Otherwise, you should leave this parameter blank.
Agent Hierarchy Group Level (AHGFilterLevel)	0	The Agent Hierarchy Group Level on which agent events should be filtered (must be between 0 and 5). Configuring a value of 0 disables filtering. Configuring a value between 1 and 5 means that agent events will be

Parameter label (name)	Default	Description
		filtered based on that Agent Hierarchy Group Level.
Agent Hierarchy Group filter value separator (AHGFilterSeparator)	,	Character used to separate matching values listed in AHGFilterValues. You should configure a separator character that does not appear in any of the individual matching values.
Agent Hierarchy Group filter matching values (AHGFilterValues)		An optional list of matching Agent Hierarchy Group Level values. If you enable Agent Hierarchy Group filtering, any agent events with an Agent Hierarchy Group Level value matching one of the values listed here will be sent on to Real-Time Adherence and any agent events that do not match the filter will be discarded. Matching values should be separated with the character configured in AHGFilterSeparator.

IAM Configuration

Parameter label (name)	Default	Description
Authorization Mode (AuthorizationMode)	User	Select User to create an IAM User for RTA. Select Role to create an IAM Role for RTA. If RTA is running outside of AWS, you should select User. If RTA is running inside AWS, you should select Role.
Source AWS Account ID (SourceAwsAccountId)		Optional AWS account ID to include in the trust policy for the IAM Role. The AWS account ID should match the AWS account from which RTA will assume the role. This parameter is required when Authorization Mode is Role. This parameter will be ignored when Authorization Mode is User.
External ID (ExternalId)		Optional external ID to include in the trust policy for the IAM Role. If Authorization Mode is Role, the role will be configured to require this external ID. You will need to configure RTA to supply this external ID when it assumes the role. If Authorization Mode is User, this parameter will be ignored.

Deployment Configuration

Parameter label (name)	Default	Description
Deployment S3 Bucket Name (DeploymentS3BucketName)	aspect-workforce	S3 bucket for the deployment assets, An S3 bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Deployment S3 Key Prefix (DeploymentS3KeyPrefix)	aspect-workforce-connect-integration/	S3 key prefix for the deployment assets. Deployment key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Option 6: Deploying Aspect Agent Productivity and Real-Time Adherence with an Existing Kinesis Data Stream

View template

Aspect Workforce™ Configuration

Parameter label (name)	Default	Description
Kinesis Firehose Stream Name (FirehoseStreamName)	aspect-wfm-ap-kda-to-s3	Enter the name of the Kinesis Firehose stream to create. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). If you have multiple Amazon Connect instances in your AWS account, you will need to create a Kinesis Firehose stream for each Amazon Connect instance and give each stream a unique name. The name of the Kinesis Firehose stream determines the filenames of agent productivity report files written to S3. By default, WFM Adapter expects the report files to be named based on a Kinesis Firehose stream name of "aspect-wfm-ap-kda-to-s3". If you specify a different stream name, be sure to update the WFM Adapter configuration for the corresponding data source to match your stream name, in the Firehose Report Mapping data source parameter. Consult the WFM Adapter help for more information.
Agent Productivity Report Prefix (ApDataS3Prefix)	OUTPUT/	Enter the prefix for Agent Productivity reports written to S3. You should

Parameter label (name)	Default	Description
		configure the corresponding WFM Adapter data source to match this value, in the Firehose Report Root Path data source parameter.
Agent Status Name Separator (StatusSeparator)	,	Character used to separate signed-out agent status names. You should configure a separator character that does not appear in any of the individual names
Signed-Out Agent Status Names (SignedOutStatuses)		Enter the list of agent status names for agent statuses that should be treated as signed-out in WFM. For example, an agent status named Break which agents use during a scheduled break would typically be listed here. Multiple signed-out agent status names may be listed. Names should be separated by the configured Agent Status Name Separator. The agent status with a Type of OFFLINE, by default named Offline, will always be treated as signed-out.
Number of SQS Queues (NumSQSQueues)	1	The number of SQS queues to create (must be between 1 and 10). Creating additional SQS queues can reduce the latency of state changes.
Write to SQS Flag Location (LambdaConfigLocation)	env	Once RTA reads an initial set of states from the agent event DynamoDB table, it toggles a Write to SQS flag to ensure that agent events are written to the SQS queue(s). This setting controls where that Write to SQS flag is stored either in an environment variable of the RTA Lambda (env) or in a configuration DynamoDB table (tab). Storing this flag in an environment variable of the Lambda requires less overhead but requires greater permissions for the RTA user. Storing this flag in a configuration DynamoDB table requires fewer permissions for the RTA user but requires an additional DyanmoDB read each time the RTA Lambda executes. By default, this flag will be stored in an environment variable of the RTA Lambda.

Amazon Connect Configuration

Parameter label (name)	Default	Description
Amazon Connect Metric Source	S3	Select S3 if WFM Adapter should calculate statistics by querying Exported S3 reports. Select API if WFM Adapter should calculate statistics by calling Connect web services. If you select S3, you should create an Amazon Connect data source in the WFM Adapter UI. If you select API, you should create an Amazon Connect (API) data source in the WFM Adapter UI.
Amazon Connect Exported Reports Bucket (ConnectS3Bucket)		Enter the name of the Exported reports S3 bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Prefix (ConnectS3Prefix)	connect/directory/Reports/Aspect/	Enter the prefix under which the exported reports read by WFM Adapter will be exported, in the Exported reports bucket of your Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is S3.
Amazon Connect Exported Reports Bucket KMS Key ARN (ConnectS3KmsArn)		(Optional) Amazon Resource Name (ARN) of the KMS key required to decrypt the exported reports of your Amazon Connect instance. You should supply this ARN if you configured your exported reports bucket to use server-side encryption with a customer-managed customer master key (CMK). Otherwise, you should leave this parameter blank.
Amazon Connect Instance ARN		Amazon Resource Name (ARN) of the Amazon Connect instance. This parameter is required if Amazon Connect Metric Source is API.
Agent Event Kinesis Stream ARN (AgentEventStreamArn)	(requires input)	Enter the Amazon Resource Name (ARN) of the Amazon Kinesis Data Stream to which Amazon Connect delivers Agent Events.
Agent Event Kinesis Stream KMS Key ARN (AgentEventStreamKmsArn)		(Optional) Amazon Resource Name (ARN) of the KMS key required to decrypt agent events. You should supply this ARN if you configured your Agent Event Kinesis stream to use server-side encryption with a customer-

Parameter label (name)	Default	Description
		managed customer master key (CMK). Otherwise, you should leave this parameter blank.
Agent Hierarchy Group Level (AHGFilterLevel)	0	The Agent Hierarchy Group Level on which agent events should be filtered (must be between 0 and 5). Configuring a value of 0 disables filtering. Configuring a value between 1 and 5 means that agent events will be filtered based on that Agent Hierarchy Group Level.
Agent Hierarchy Group filter value separator (AHGFilterSeparator)	,	Character used to separate matching values listed in AHGFilterValues. You should configure a separator character that does not appear in any of the individual matching values.
Agent Hierarchy Group filter matching values (AHGFilterValues)		An optional list of matching Agent Hierarchy Group Level values. If you enable Agent Hierarchy Group filtering, any agent events with an Agent Hierarchy Group Level value matching one of the values listed here will be sent on to Real-Time Adherence and any agent events that do not match the filter will be discarded. Matching values should be separated with the character configured in AHGFilterSeparator.

IAM Configuration

Parameter label (name)	Default	Description
Authorization Mode (AuthorizationMode)	User	Select User to create IAM Users for WFM Adapter and RTA. Select Role to create IAM Roles for WFM Adapter and RTA. If WFM Adapter and RTA are running outside of AWS, you should select User. If WFM Adapter and RTA are running inside AWS, you should select Role.
Source AWS Account ID (SourceAwsAccountId)		Optional AWS account ID to include in the trust policy for the IAM Role. The AWS account ID should match the AWS account from which WFM Adapter and RTA will assume their roles. This parameter is required when Authorization Mode is Role. This parameter will be ignored when Authorization Mode is User.

Parameter label (name)	Default	Description
External ID (ExternalId)		Optional external ID to include in the trust policy for the IAM Role. If Authorization Mode is Role, the role will be configured to require this external ID. You will need to configure WFM Adapter and RTA to supply this external ID when they assume their roles. If Authorization Mode is User, this parameter will be ignored.

Deployment Configuration

Parameter label (name)	Default	Description
Deployment S3 Bucket Name (DeploymentS3BucketName)	aspect-workforce	S3 bucket for the deployment assets, An S3 bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Deployment S3 Key Prefix (DeploymentS3KeyPrefix)	aspect-workforce-connect-integration/	S3 key prefix for the deployment assets. Deployment key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

Step 4. Enable Data Streaming

If you selected a deployment option that created a Kinesis data stream, follow the steps in the Amazon Connect documentation to set up Data Streaming and enable Agent Event streaming to the Kinesis stream created by the integration. The Amazon Resource Name (ARN) of the Kinesis stream created will be listed in the Outputs of the CloudFormation stack for the integration. The ARN will be listed as the value of the output with a key of “AgentEventStreamARN.”

Step 5. Test the Deployment

In previous versions of the Agent Productivity integration, some post-deployment configuration was required. In this version of the Agent Productivity integration, this post-deployment configuration is no longer required. The Agent Productivity Lambda should begin working as soon as Amazon Connect writes any agent events to the agent event stream.

If you add any new agent statuses that should be treated as signed-off, you should configure those in the SignedOffAgentStatuses environment variable of the Lambda function identified by the APKinesisLambdaFunctionName output of your deployment.

If you chose an option that includes Agent Productivity, you will need to configure the Aspect WFM Adapter product to test your deployment. Consult the Aspect WFM Adapter documentation for more information

If you chose an option that includes Real-Time Adherence, you will need to configure the Aspect Real-Time Adherence product to test your installation. Consult the Aspect Real-Time Adherence product documentation for details.

Best Practices Using Aspect Workforce™ on AWS

Deployment options that include Agent Productivity create an S3 bucket to hold agent sign-in/sign-out information. Once this bucket is created, you should configure lifecycle rules that are consistent with your policies for other S3 buckets in your AWS account. Consult the Amazon S3 documentation for more information.

Keep in mind that lifecycle rules may affect that your ability to reship reports in Aspect WFM Adapter. You will be limited to the date/time range for which objects are stored in both the S3 bucket created by Aspect Agent Productivity and the Exported reports bucket associated with your Amazon Connect instance (for the Amazon Connect data source type) or the date/time range for which metrics are stored in Amazon Connect (for the Amazon Connect (API) data source type). Make sure that your lifecycle rules persist objects during the window of time for which you would like to be able to reship reports.

Both the Agent Productivity and Real-Time Adherence features read from the Agent Event Kinesis data stream of your Amazon Connect instance. If you selected a deployment option that created this Kinesis data stream, the Kinesis data stream will be created with a default shard count of 1. You may need to increase the shard count for the stream to support the Agent Productivity and/or Real-Time Adherence features of Aspect Workforce™, whether the stream was created by this integration or not. When you size the stream, you need to consider both:

- The amount of data you expect to be written. Amazon Connect writes to the stream when agents change state.
- The amount of data you expect to be read. If you included Agent Productivity support, the corresponding Kinesis Data Lambda function will read from the stream. If you included Real-Time Adherence support, the corresponding RTA Lambda function will read from the stream. You may need to deploy multiple instances of the RTA Lambda function, if you wish to monitor agents an Amazon Connect instance on multiple Real-Time Adherence servers. In addition, you may have other custom applications that read from the stream.

Consult the Amazon Kinesis documentation for more information.

Security

The deployment options for this integration include a new parameter, Authorization Mode, which specifies whether the integration should create IAM users or IAM roles for Aspect WFM Adapter and/or Aspect Real-Time Adherence (RTA). In general, we recommend that you create IAM users if WFM Adapter and/or RTA is running outside of AWS and create IAM roles if WFM Adapter and/or RTA is running inside of AWS. The following configuration options are available for WFM Adapter and RTA:

1. A checkbox that specifies whether to use implicit AWS credentials. Both WFM Adapter and RTA use the AWS SDK for .NET to access AWS. See Credential and profile resolution for more information about configuring implicit credentials. If WFM Adapter and/or RTA is running on an Amazon EC2 instance, you can use the IAM identity associated with the EC2 instance (the IAM Role specified in the EC2 instance metadata) as a source of implicit credentials. If the checkbox is not checked, you must supply the following values:

    a. Access key ID – a programmatic username for the corresponding IAM user.

    b. Secret access key – a programmatic password for the corresponding IAM user.

    c. See below for more information about creating AWS access keys.

2. A checkbox that specifies whether to assume a role. If this checkbox is not checked, The permissions required must be associated with the IAM identity above: either the IAM identity associated with the implicit credentials or the IAM identity associated with the configured AWS access key. If this checkbox is checked, you must supply the following values:

    a. The Amazon Resource Name (ARN) of the role to assume. The ARNs of any IAM roles created will be listed in the Outputs of the CloudFormation stack. If the integration includes Agent Productivity, the Outputs will include WFMAdapterRoleARN. If the integration includes RTA, the Outputs will include RTARoleARN.

    b. The external ID to supply when assuming the role. The external ID is an extra security measure to limit access to the role. When you deploy the integration, you must specify an external ID. The external ID should be a value that identifies you as an Aspect customer, e.g., your customer ID. If you do not remember the external ID you configured when deploying the integration, check the Parameters tab of the CloudFormation stack.

These configuration options can be used to support the following scenarios:

3. WFM Adapter and/or RTA are installed on a machine running outside of AWS.

    a. Authorization mode is User – in this case, the IAM user(s) created by the integration have the required permissions. You will need to create an AWS access key for each IAM user. You should not configure WFM Adapter and/or RTA to assume a role.

        i. Implicit credentials – configure the AWS access key in one of the supported credential locations, e.g., the AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY environment variables. If you rotate the access keys, you just need to update them in the implicit credential location, rather than the WFM Adapter and/or RTA configuration UI.

ii. Explicit credentials – configure the AWS access key in the WFM Adapter/RTA configuration UI. If you rotate the access keys, you will need to update them in the WFM Adapter/RTA configuration UI.

b. Authorization mode is Role – in this case, the IAM role(s) created by the integration have the required permissions. You should configure WFM Adapter and/or RTA to assume a role. You will need to supply the ARN of the corresponding role and the external ID in the WFM Adapter/RTA configuration UI. You will also need to create a corresponding IAM user for each of the IAM roles. However, the only permission required for the new IAM user is sts:AssumeRole access to the corresponding IAM role. The main advantage of this approach is that it limits the permissions associated with AWS access keys. An attacker who compromised the AWS access key of a user would also need to know the role ARN and the external ID to be able to access any AWS resources. Note: the Source AWS Account ID you specify when deploying the integration should match the AWS account containing the new IAM user(s).

i. Implicit credentials – configure the AWS access key in one of the supported credential locations, e.g., the AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY environment variables. If you rotate the access keys, you just need to update them in the implicit credential location, rather than the WFM Adapter and/or RTA configuration UI.

ii. Explicit credentials – configure the AWS access key in the WFM Adapter/RTA configuration UI. If you rotate the access keys, you will need to update them in the WFM Adapter/RTA configuration UI.

4. WFM Adapter and/or RTA are installed on an EC2 instance running inside of AWS.

a. Authorization Mode is User – this option is not recommended. However, if you need to use this option, follow the instructions above for running outside of AWS.

b. Authorization Mode is Role – in this case, the IAM role(s) created by the integration have the required permissions. You will need to update the IAM role associated with the EC2 instance to grant sts:AssumeRole permission to the IAM role(s) created. The Source AWS Account ID you specify when deploying the integration should match the AWS account containing the EC2 instance. You should configure WFM Adapter and/or RTA as follows:

i. Use implicit credentials.

ii. Assume a role. Supply the ARN of the corresponding role. Supply the external ID.

c. Note: it is also possible to grant the permissions required by WFM Adapter and/or RTA directly to the IAM role associated with the EC2 instance. This is not recommended, since it would provide access to any applications running on that EC2 instance.

If you create an Amazon Connect data source, the Aspect WFM Adapter product requires read-only access to two S3 buckets:

- The Exported reports bucket of your Amazon Connect instance
- The S3 bucket created by this deployment

If you create an Amazon Connect (API) data source, the Aspect WFM Adapter product requires the following access:

- Read-only access to the S3 bucket created by this deployment
- Access to call Connect web services for your Amazon Connect instance. The following Connect permissions are required: connect:DescribeUserHierarchyGroup, connect:GetMetricDataV2,

connect:ListQueues, connect:ListRoutingProfiles, connect:ListUsers, and connect:SearchUserHierarchyGroups.

If the integration includes Agent Productivity, it will create an IAM user or IAM role with the minimum permissions required by Aspect WFM Adapter.

The Aspect Real-Time Adherence (RTA) product requires access to the following:

- The DynamoDB table that holds the last state change of each signed-in agent. RTA needs read-only access to this table.
- The SQS queue(s) that are used to relay agent events to RTA. RTA needs to be able to read and delete entries from these SQS queue(s).
- If configuration information is stored in a table, the configuration DynamoDB table. RTA needs to be able to read and update this table.
- Otherwise, the configuration of the Lambda function that updates the DynamoDB table and SQS queue(s). RTA needs to be able to read and update the configuration of the Lambda function.

Aspect Real-Time Adherence updates the configuration DynamoDB table or an environment variable to instruct the Lambda function to start writing agent events to the SQS queue(s), after it reads the contents of the DynamoDB table.

If the integration includes Real-Time Adherence, it will create an IAM user or IAM role with the minimum permissions required by Aspect Real-Time Adherence.

To grant access to an IAM user, you will need to create an access key for the user. To do so:

1. Select the IAM Service in the AWS Management Console.
2. Select **Users**.
3. Select the User created by this integration. To determine the user name, check the Outputs of the CloudFormation stack. The WFM Adapter user name will be listed as the value of the output with a key of **WFMAdapterUserName**. The RTA user name will be listed as the value of the output with a key of **RTAUserName**.
4. Select the **Security credentials** tab.
5. Under the **Access Keys** section, press the **Create access key** button.
6. On the **Access key best practices & alternatives** page, select **Application running outside AWS** and click **Next**.
7. On the **Set description tag** page, enter description if desired and click **Create Access Key**.
8. Click **Download .csv file** to save the **Access Key** and **Secret Access Key** values. (Once you leave this page you will not be able to retrieve them again without generating a new pair.)

When the integration creates an IAM role, it creates a trust policy for the role that includes:

- The Source AWS Account ID. If Source AWS Account ID refers to a different AWS account than the current AWS account, this grants remote access to assume the role by IAM identities in the source AWS account. If you are an Aspect Public Cloud customer running in AWS, this should be the AWS account ID of the Aspect Public Cloud account containing your instance. Check with your Aspect Customer Support representative to obtain this AWS account ID.
- A condition that matches the External ID. Any AssumeRole request that doesn't include the correct external ID will be rejected.

In addition, the IAM identity that assumes the role, needs to have sts:AssumeRole access to the role. You will need to grant this access by hand. This integration will not grant that access, since it does not know which IAM identities require access and those IAM identities may be in a different AWS account. The sts:AssumeRole permission must be configured in the source AWS account. Here is an example of a policy to grant sts:AssumeRole access to an IAM role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::12345789012:role/RoleName"
      ]
    }
  ]
}
```

If you are an Aspect Public Cloud customer running in AWS, contact Aspect Customer Support after deploying this integration. You will need to provide the ARN(s) of the role(s) created so that Aspect can grant access to assume the role(s) from the Aspect Public Cloud AWS account.

If you enable server-side encryption on either the Exported reports S3 bucket of your Amazon Connect or the Agent event Kinesis stream of your Amazon Connect, you may need to supply the ARN of the corresponding KMS key during deployment. Server-side encryption can be configured in several ways. If you use a customer managed KMS master key, additional permissions will be required to grant the integration object access to decrypt data from that resource. If AWS is responsible for managing the KMS master key, no additional permissions are required.

By default, the S3 bucket created when you create an Amazon Connect instance is configured to use server-side encryption with an AWS-managed KMS master key (called aws/connect). If you use the default AWS-managed KMS master key, you do not need to supply a value for the Amazon Connect Exported Reports Bucket KMS Key ARN parameter when you deploy the integration. If you configure your Amazon Connect to encrypt exported reports using a KMS master key that you created, you should supply the ARN of that KMS master key as the value of the Amazon Connect Exported Reports Bucket KMS Key ARN parameter when you deploy the integration.

By default, Amazon Connect does not support encrypting the contents of the Agent event Kinesis stream with a customer managed KMS master key, since, by default, Amazon Connect would not have the right to encrypt agent events using that key. However, you can work around this issue by using the same customer managed KMS master key for the Kinesis stream that you chose to use for encrypting exported reports, call recordings, or chat transcripts. In that case, you should supply the ARN of the KMS master key as the value of the Agent Event Kinesis Stream KMS Key ARN parameter when you deploy the integration. If your Agent event Kinesis stream is not configured to use server-side encryption, or you use an AWS-managed KMS master key, you do not need to supply a value for the Agent Event Kinesis Stream KMS Key ARN parameter when you deploy the integration.

Note: If you choose one of the deployment options where the integration is responsible for creating a Kinesis stream, the Kinesis stream will not be configured to use server-side encryption. If you later choose to enable server-side encryption with a customer managed KMS master key, you will need to grant the required permissions by hand. If you plan configure your Agent event Kinesis stream to use server-side encryption with

a customer managed KMS master key, Aspect recommends that you create the Kinesis stream before deploying the integration and then use one of the deployment options for an existing Kinesis stream.

FAQ

Q. I encountered a CREATE_FAILED error when I launched the integration.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template, and select the **Create change set** button. Once the changesets are created, and you click the **Execute change set** button, select the **Preserve successfully provisioned resources**. With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. (Look at the log files in %ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.)

 **Caution:** When you select **Preserve successfully provisioned resources**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS Cloudformation templates.

A. We recommend that you launch the integration templates from the location we've provided or from another S3 bucket. If you deploy the **templates** from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Git Repository

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

Additional Resources

AWS Services

- Amazon Connect
  https://aws.amazon.com/documentation/connect/
- Amazon S3
  https://aws.amazon.com/documentation/s3/
- Amazon DynamoDB
  https://aws.amazon.com/documentation/dynamodb/
- Amazon SQS
  https://aws.amazon.com/documentation/sqs/
- Amazon Kinesis
  https://aws.amazon.com/documentation/kinesis/
- AWS Lambda
  https://aws.amazon.com/documentation/lambda/
- Amazon CloudWatch
  https://aws.amazon.com/documentation/cloudwatch/
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/

License Notice

Note: The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

About Aspect®
Aspect is dedicated to transforming the service economy by humanizing the workforce experience. Their WorkforceOS platform offers a robust workforce management solution that aligns employee preferences with business needs enhancing scheduling, predictive insights, and collaboration tools. Supported by its parent company, Alvaria Inc., which boasts over 50 years of leadership in workforce management technology, Aspect is a trusted partner for large global enterprises across key sectors, including financial services, airlines, automotive, insurance, retail, telecommunications, and utilities. The Aspect WorkforceOS stands out as the only culture-driven WEM software designed to foster work-life balance while maximizing ROI for businesses. For more details, visit www.aspect.com