AWS Landing Zone

AWS Implementation Guide

November 2018

Contents

About This Guide

This implementation guide discusses architectural considerations and configuration steps for deploying the AWS Landing Zone solution on the Amazon Web Services (AWS) Cloud. It includes links to AWS CloudFormation templates that launch, configure, and run the AWS services required to deploy this solution using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting on the AWS Cloud.

Overview

Amazon Web Services (AWS) enables customers to achieve significant gains in productivity, innovation, and cost reduction when they move to the AWS cloud. AWS offers a variety of services and features that allow for flexible control of cloud computing resources and also of the AWS account(s) managing those resources. With the large number of design choices, setting up a multi-account environment can take a significant amount of time, involve the configuration of multiple accounts and services, and require a deep understanding of AWS services. In order to help customers more quickly set up secure, multi-account AWS environments based on AWS best practices, AWS offers the AWS Landing Zone solution.

This solution helps customers implement an initial security baseline by creating core accounts and resources and can help save customers time by automating the set-up of their environments for running secure and scalable workloads. The solution deploys an AWS Account Vending Machine (AVM) product for provisioning and automatically configuring new accounts, and leverages AWS Single Sign-On (SSO) for managing user account access. This environment is fully customizable to allow customers to implement their own account baselines through a Landing Zone configuration and update pipeline.

Cost

You are responsible for the cost of the AWS services used while running the AWS Landing Zone solution. As of the date of publication, the cost for running this solution with default settings in the US East (N. Virginia) Region is approximately **$200 per month**. This includes charges for AWS Config Rules, Amazon GuardDuty (assuming <1 million AWS CloudTrail events and <= 1GB of flow logs entries per month), and AWS CodePipeline. This cost estimate does not include charges for the Add-On products available.

If you choose to deploy the Centralized Logging Solution add-on product with Amazon ElasticSearch Service, the cost for running this solution with default settings is approximately **$400 per month**.

If you choose to deploy the AWS Managed AD and Directory Connector add-on product, the cost for running this solution with default settings is approximately **$340 per month**. For full details, see the pricing webpage for each AWS service you will be using in this solution.

Architecture Overview

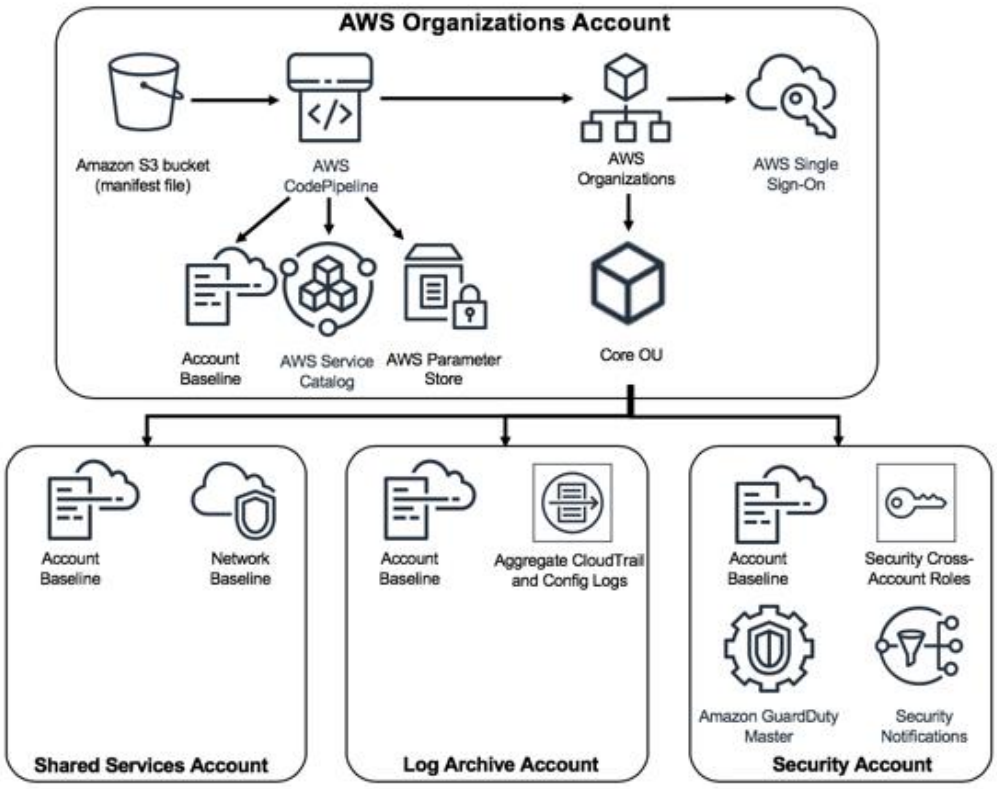


Figure 1: AWS Landing Zone architecture on AWS

The AWS CloudFormation template enables AWS Organizations in an account, creates an Amazon Simple Storage Service (Amazon S3) bucket and Landing Zone configuration zip file, an AWS CodePipeline pipeline for creating and updating the landing zone baseline, and, if requested, automatically starts the pipeline to build out the landing zone implementation.

Solution Components

AWS Organizations

AWS Organizations is enabled to allow customers to programmatically create and manage multiple AWS accounts. AWS Organizations allows customers to create groups of accounts apply policies to those groups, hosts the AWS Landing Zone account provisioning pipelines, baseline configuration workflows, and the AWS Single Sign-On (SSO) endpoint for managing user access to landing zone managed accounts.

AWS Key Management Service (KMS)

An AWS Landing Zone KMS encryption key is created for this solution (`AwsLandingZoneKMSKey`). This key is used to encrypt objects in the Amazon S3 configuration bucket and sensitive parameters in AWS Systems Manager Parameter Store. By default, only AWS Landing Zone provisioning roles have permission to perform encrypt or decrypt operations with this key. AWS Landing Zone administrators will need to be added to the `AwsLandingZoneKMSKey` policy to access the configuration file or Parameter Store SecureString values.

Amazon S3

An AWS Landing Zone Amazon S3 bucket (`aws-landing-zone-configuration-[account-id]-[region]`) and configuration zip file (`aws-landing-zone-configuration.zip`) provides a manifest and all related templates for describing and implementing a customer's landing zone environment. The manifest describes AWS account structures and dependencies required to implement a customer's account baseline for new and existing accounts. Updating this configuration file triggers the AWS Landing Zone configuration pipeline.

See the AWS Landing Zone User Guide for more detailed information about the solution and the AWS Landing Zone Developer Guide for more detailed information about customizing the solution.

AWS Single Sign-On (SSO)

Providing least-privilege, individual user access to your AWS accounts is an essential, foundational component to AWS account management. The default landing zone implementation deploys SSO with AWS SSO directory where users and groups can be managed in SSO. The solution also allows customers to deploy the AWS Managed Active Directory (AD) and Directory Connector add-on product. For more information see the AWS Landing Zone Developer Guide.

AWS CodePipeline

AWS CodePipeline is a continuous integration and continuous delivery service for fast and reliable application and infrastructure updates. AWS CodePipeline is used to validate, test, and implement AWS Landing Zone changes based on updates to the configuration zip file in Amazon S3. The pipeline includes stages to validate and manage the Landing Zone configuration files and templates, core accounts, AWS Organizations Service Control Policies (SCPs), AWS Service Catalog portfolios and products, and AWS CloudFormation StackSets. It also manages and updates an AWS Service Catalog Account Vending Machine (AVM) product for creating new accounts and implementing account configuration baselines. For more information about the pipeline stages, see the AWS Landing Zone Developer Guide.

AWS CloudFormation StackSets

This solution leverages AWS CloudFormation StackSets, a collection of AWS resources that you can manage as a single unit, to enable you to create, update, or delete stacks across multiple accounts and AWS Regions. AWS Landing Zone StackSets are deployed by AWS CodePipeline and used to create core account resource dependencies and baseline AWS accounts. Stack instances are deployed using the AWS Organization preconfigured role (`AWSCloudFormationStackSetExecutionRole`).

AWS Service Catalog

AWS Service Catalog allows IT administrators to create, manage, and distribute catalogs of approved products to end users, and access the products using a self-service portal. AWS Landing Zone leverages AWS Service Catalog to provide an Account Vending Machine (AVM) product to allow customers to easily add and baseline new accounts to their AWS environment. AWS Service Catalog is also used to deploy optional components, such as an Amazon Elasticsearch-based log analytics tool.

AWS Systems Manager Parameter Store

AWS Systems Manager Parameter Store is used to store AWS Landing Zone configuration parameters. These parameters are used for integrating related configuration templates, such as configuring each account to log AWS CloudTrail data to a centralized Amazon S3 bucket. Additionally, AWS Landing Zone administrators can leverage the Systems Manager Parameter Store to view AWS Landing Zone input and parameters in one centralized location.

Implementation Considerations

AWS Landing Zone Initial Deployment

When setting up an AWS Landing Zone, customers can choose when they would like their landing zone to be deployed. By default, this solution will create and run the solution through an AWS Landing Zone Configuration Pipeline. Three AWS core accounts are created to store archive logs, provide emergency security access, and host shared services. For more information, see the AWS Landing Zone User Guide.

Customers who don't want the three accounts to be created, or would like to modify the solutions core resources before it's run through the pipeline, the initialization template provides the following two options:

- **Auto Build Landing Zone:** This input parameter controls if the AWS Landing Zone solution will automatically be built and deployed by the landing zone configuration pipeline. Keeping the default parameter `Yes`, the initialization CloudFormation stack will copy the implementation to the customer's AWS Landing Zone configuration Amazon S3 bucket with the name `aws-landing-zone-configuration.zip`. This will automatically trigger the AWS Landing Zone Configuration Pipeline.

  Modifying the **Auto Build Landing Zone** parameter to `No`, will keep the AWS Landing Zone Configuration Pipeline from executing by prepending an underscore character to the implementation configuration zip file (`_aws-landing-zone-configuration.zip`). This allows configuration changes to be made before executing the AWS Landing Zone Configuration Pipeline. Once you are ready to execute the configuration pipeline, rename the file to remove the prepended underscore, or upload a new file called `aws-landing-zone-configuration.zip`.

- **Pipeline Approval Stage:** This input parameter determines if manual approval is required in the AWS Landing Zone Configuration Pipeline before deploying configuration changes. When enabled, the configuration pipeline will validate the AWS Landing Zone configuration file manifest and templates, and pause for manual approval before executing the rest of the pipeline stages that implement the AWS Landing Zone. The parameter can be used initially to keep the AWS Landing Zone configuration from executing by rejecting the first attempt to run through the pipeline. It can also be used for manual validation of AWS Landing Zone configuration changes as a final control before implementation.

Cross-Account Roles

AWS Landing Zone repurposes the AWS Organizations created preconfigured role for landing zone provisioning (`AWSCloudFormationStackSetExecutionRole`). By default, AWS Landing Zone will lock down access to this role to AWS Landing Zone provisioning roles as a recommended security best practice. Locking down access creates a dependency between specific roles in the AWS Organization account and the preconfigured role in member accounts.

> **Note**: Do NOT terminate the AWS Landing Zone initialization template unless you have provisioned alternative access to member accounts such as setting up AWS SSO. Terminating without setting up alternative access will delete the provisioning roles, and you will need to reset the root password reset to gain access to member accounts.
>
> We recommend enabling Stack Termination protection to prevent accidental initialization template deletion.

Configuration Zip file in Amazon S3

When setting up the AWS Landing Zone solution, customers can change the configuration ZIP file stored in the Amazon Simple Storage Service (Amazon S3) bucket in the master account. The file is protected using Server-Side Encryption (SSE) with AWS Key Management Service (AWS KMS), and denial of use of the KMS key by users. To access the file, the KMS Key Policy must be updated with administrator role or user name.

1. In the AWS Management Console, navigate to the **IAM console**.
2. In Encryption Keys, select the **AwsLandingZoneKMSKey**
3. In the Allow Use of the Key section, update the **Key Policy**
   - To add an administration role, add the following Principal: **`arn:aws:iam::<account ID>:role/<administrator role>`**
   - To add a user, add the following Principal: **`arn:aws:iam::<account ID>:user/<username>`**"
4. Select **Save Changes**
5. Navigate to the **Amazon S3 bucket** in the master account, and download the **configuration ZIP file**.

Once all of the necessary configuration changes are made to the manifest file and template files, upload your changes using the following procedure:

1. Zip the modified configuration files, and name the file: **aws-landing-zone-configuration-<account ID>-<region>.zip**
2. Upload the file to Amazon S3 using SSE with AWS KMS master-key: **AwsLandingZoneKMSKey**

Note that uploading the file without the underscore prefix in the file name will automatically execute the Landing Zone pipeline configuration updates.

AWS CloudFormation Template

This solution uses AWS CloudFormation to automate the deployment of the AWS Landing Zone solution on the AWS Cloud. It includes the following AWS CloudFormation template:

View template **aws-landing-zone-initiation.template:** This template deploys AWS Organizations, an Amazon Simple Storage Service (Amazon S3) bucket with an AWS Landing Zone configuration zip file, and AWS CodePipeline, but can also be customized to fit your needs.

Automated Deployment

Before you launch the automated deployment, please review the architecture, configuration, network security, and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the AWS Landing Zone solution into your account.

Time to deploy: Approximately five minutes for the solution initiation template, and one-hour for the implementation.

Prerequisites

This solution is designed to be run in a brand new AWS account, with a completed Service Limit increase for a minimum of **10** AWS accounts in AWS Organizations. We also recommend submitting a Service Limit increase for 50 AWS CloudFormation StackSets.

What We'll Cover

BIG NOTE: Delete default VPCs first. AVM might not be able to delete them because it prompts the user if OK to delete the default VPC

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 values for the required template parameters.
- Review the other template parameters and adjust if necessary.

Step 2. Enable AWS CloudFormation Stack Termination Protection

- Enable AWS CloudFormation stack termination protection to prevent accidental stack deletion.

Step 3. AWS Landing Zone Implementation

- Review the landing zone implementation and AWS Landing Zone configuration pipeline.

Step 1. Launch the Stack

This automated AWS CloudFormation template deploys the AWS Landing Zone solution on the AWS Cloud.

1. Log in to the AWS Management Console and click the button to the right to launch the `aws-landing-zone-initiation` AWS CloudFormation template.
   You can also download the template as a starting point for your own implementation.

2. The template is launched 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 services, which are currently available in specific AWS Regions only. Therefore, you must launch this solution in an AWS Region where these services are available. [1]

3. On the **Specify Details** page, assign a name to your solution stack.
4. Under **Parameters**, review the parameters for the template and modify them as necessary. This solution uses the following default values.

Landing Zone Account Configuration		
Parameter	**Default**	**Description**
Shared Services Account Email Address	*<Requires input>*	Email address used to create a centralized Shared Services account
Log Archive Account Email Address	*<Requires input>*	Email address used create a centralized log archive account

[1] For the most current service availability by AWS Region, see https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

Landing Zone Account Configuration		
Security Account Email Address	*<Requires input>*	Email address used create a centralized security account
Security Alert Email Address	*<Requires input>*	Email for all the Security Alerts related to Landing Zone.
Subscribe All Change Events Email to Topic	No	Subscribe an email address to an Amazon SNS topic for all managed account AWS CloudTrail and AWS Config change events.
All Change Events Email	<Optional Input>	Optional email address to subscribe to all change events
Core OU Name	core	Name of Organizations Unit for the Core Accounts.
Non Core OU Names	applications	Comma separated list of additional Organizations Unit names for organizing additional AWS accounts by applications, business units, etc.

Landing Zone Pipeline Configuration		
Parameter	Default	Description
Pipeline Approval Stage	No	Do you want to add a manual approval stage to the AWS Landing Zone Configuration Pipeline?
Pipeline Approval Email Address	<Optional input>	Email for notifying that the Landing Zone pipeline is waiting for an Approval. This parameter is not required if you selected `No` to the **Pipeline Approval Stage** parameter.
Auto Build Landing Zone	Yes	Choose if you want to trigger the pipeline right away to build the Landing Zone.
Lock StackSetsExecution Role	Yes	Locks down the AWS StackSets Execution role in the member accounts to only allow access from provisioning roles.

Shared Services Configuration		
Parameter	**Default**	**Description**
Shared Services VPC Options	Shared-Services-Network-3-AZs	Create a shared service VPC with subnets in 2 or 3 AZs. The 3 AZ option is recommended for all regions except when the desired AD Region only has 2 AZs.
Shared Services VPC CIDR	100.64.0.0/16	CIDR block for the Shared Services VPC, which will include AWS Managed Microsoft AD. You can modify the address range to avoid overlapping with existing networks.

AWS Config		
Parameter	**Default**	**Description**
Enable AWS Config All Regions	Yes	Choose if you want AWS Config service and rules in all AWS Regions.

AWS Config Rules		
Parameter	**Default**	**Description**
Enable Encrypted Volume Rule	Yes	Enables the AWS managed encrypted-volumes config rule. To disable, change the parameter value to No.
Enable RDS Encryption Rule	Yes	Enables the AWS managed rds-storage-encrypted config rule. To disable, change the parameter value to No.
Enable S3 Public Read Rule	Yes	Enables the AWS managed s3-bucket-public-read-prohibited config rule. To disable, change the parameter value to No.
Enable S3 Public Write Rule	Yes	Enables the AWS managed s3-bucket-public-write-prohibited config rule. To disable, change the parameter value to No.
Enable S3 SSE Policy Rule	No	Enables the AWS managed s3-bucket-server-side-encryption-enabled config rule. To enable, change the parameter value to Yes.
Enable Root MFA Rule	Yes	Enables the AWS managed root-account-mfa-enabled config rule. To disable, change the parameter value to No.
Enable IAM Password Policy Rule	Yes	Enables the AWS managed iam-password-policy config rule. To disable, change the parameter value to No.
Enable Restricted Common Ports Rule	Yes	Enables the AWS managed restricted-common-ports config rule. To disable, change the parameter value to No.
Enable Restricted SSH Rule	Yes	Enables the AWS managed restricted-ssh config rule. To disable, change the parameter value to No.

VPC Flow Logs Retention Policy		
Parameter	**Default**	**Description**
VPC Flow Logs Retention in Days	90	Specifies the number of days you want to retain VPC flow logs in each account.

5. Choose **Next**.
6. On the **Options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.

8. Choose **Create** to deploy the stack.
9. You can view the status of the stack in the AWS CloudFormation Console in the **Status** column. You should see a status of CREATE_COMPLETE in approximately five minutes.

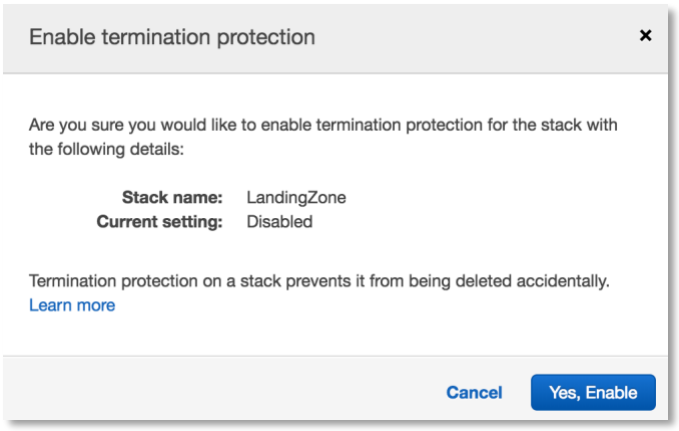
Step 2. Enable AWS CloudFormation Stack Termination Protection

The AWS Landing Zone initialization template creates `account provisioning` and `configuration cross-account` roles that are essential to managing your landing zone when locking down the default **StackSets ExecutionRole**.

> **Note:** Only terminate the AWS Landing Zone initialization template if you have provisioned alternative access for managing your member accounts.

To help prevent against accidental termination of your initialization template, AWS recommends enabling AWS CloudFormation termination protection by using the following procedure:

1. Select your **AWS Landing Zone stack**.
2. In the **Actions** menu, select **Change termination protection**, and select **Yes, Enable**.



Step 3. AWS Landing Zone Implementation

The initiation template will create an AWS Landing Zone configuration Amazon S3 bucket (`aws-landing-zone-configuration-[account-id]-[region]`), configuration ZIP file (`aws-landing-zone-configuration.zip`), and an AWS CodePipeline and AWS Step Functions for implementing AWS Landing Zone configuration changes.

By default, the input parameter **Auto Build Landing Zone** will trigger the AWS CodePipeline to process the configuration ZIP file and deploy the solution. If you selected **No** to the input parameter **Auto Build Landing Zone**, the implementation will not deploy automatically. When you are ready to deploy the implementation, you will need to remove the prepended (_) from the file `_aws-landing-zone-configuration.zip` or upload a new copy of the configuration file with the name `aws-landing-zone-configuration.zip`.

Deploying the implementation takes approximately one hour. While the pipeline is executing, you can follow these steps to explore the AWS Landing Zone deployment and configuration process.

1. Navigate to the **IAM console**, select the **Encryption keys** option on the left, and select the **Get Started** button (if applicable).
2. Select the AWS Region where you launched the initialization template, and select the **AwsLandingZoneKMSKey**.
3. Modify the **Key Policy** to add any Landing Zone administrators to the **Allow use of the key** section.

   The following example allows the root user, or any IAM principal in the account with KMS encrypt or decrypt permissions to use this key:

   Note that AWS recommends restricting this key policy to an AWS administrator role once that is defined for your company.

```
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<account>:root",
          "arn:aws:iam::<account>:role/LandingZoneCodePipelineRole",

"arn:aws:iam::<account>:role/StateMachineTriggerLambdaRole",

"arn:aws:iam::<account>:role/LandingZoneDeploymentLambdaRole",
          "arn:aws:iam:: <account>:role/StateMachineLambdaRole",
          "arn:aws:iam:: <account>:role/LandingZoneLambdaRole"
        ]
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
```

```
            "kms:DescribeKey"
        ],
        "Resource": "*"
    }
```

4. Navigate to the Amazon S3 console, browse the configuration bucket, download, extract, and browse the configuration ZIP file contents.
5. Navigate to the **AWS CodePipeline** console, and select the **AWS-Landing-Zone-Codepipeline** pipeline.

   Viewing the pipeline will allow you to see the status and execution details for each pipeline stage. For more information about the AWS Landing Zone pipeline, see the AWS Landing Zone Developer's Guide.

   If you selected **Yes** for the input parameter **Pipeline Approval Stage**, you will need to use the AWS CodePipeline console to manually approve the AWS Landing Zone deployment.
6. Navigate to the **Step Functions console**.

   You will see a list of the AWS Landing Zone state machines as well as a summary of state machine executions. As the pipeline executes, state machines will run and enter either a succeeded or failed state. Selecting each state machine will show the execution status and details for each state machine execution, including the ability to view the inputs, outputs, and exceptions for each state machine state. Use this to troubleshoot pipeline stage failures by locating the appropriate state machine and looking for failed executions.
7. Navigate to the **CloudFormation StackSets** console to view the AWS Landing Zone configuration StackSets and StackSet instances.
8. Navigate to the **AWS Systems Manager Parameter Store** console to view the AWS Landing Zone parameters.
9. Navigate to the **AWS Service Catalog** console to view AWS Landing Zone portfolios (AWS Landing Zone - Baseline, AWS Landing Zone - Core), the AVM product, and optional products. For information about using the AVM and installing and configuring optional products, see the AWS Landing Zone User Guide.
10. Navigate back to the **AWS CodePipeline console** and verify the pipeline has completed successfully.

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.

Appendix A: Collection of Anonymous Data

This solution includes an option to send anonymous usage data to AWS. We use this data to better understand how customers use this solution and related services and products. When enabled and Amazon Inspector is deployed, the following information is collected and sent to AWS:

- **Solution ID:** The AWS solution identifier
- **Unique ID (UUID):** Randomly generated, unique identifier for each solution deployment
- **Timestamp:** Data-collection timestamp
- **Managed Instance Count:** The number of Amazon Inspector Agents within the Assessment Run

Note that AWS will own the data gathered via this survey. Data collection will be subject to the AWS Privacy Policy. To opt out of this feature, complete one of the following tasks:

a) Modify the AWS CloudFormation template mapping section as follows:

```
Solution:
Metrics:
SendAnonymousData: ”Yes”
```

to

```
Solution:
Metrics:
SendAnonymousData: “No”
```

OR

b) After the solution has been launched, find the `/org/primary/metrics_flag` SSM parameter key in the Parameter store console and set the value to `No`.

Send Us Feedback

We welcome your questions and comments. Please post your feedback on the AWS Solutions Discussion Forum.

Document Revisions

Date	Change	In sections
November 2018	*Initial Release*	--

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS 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.

The AWS Landing Zone solution is licensed under the terms of the Amazon Software License available at https://aws.amazon.com/asl/.