

AWS Landing Zone

AWS User Guide

June 2018



Copyright (c) 2018 by Amazon.com, Inc. or its affiliates.

AWS Landing Zone User Guide is licensed under the terms of the Amazon Software License available at

<https://aws.amazon.com/asl/>

Contents

| | |
|--|----|
| Overview | 3 |
| Considerations..... | 3 |
| AWS Landing Zone Configuration | 4 |
| AWS Accounts | 4 |
| Organization Account | 4 |
| Shared Services Account..... | 5 |
| Logging Account | 5 |
| Security Account | 5 |
| Security Notification Architecture | 5 |
| Security Baseline | 6 |
| Account Vending Machine Architecture | 8 |
| AVM Permissions | 9 |
| Creating New Accounts | 9 |
| Step 1. Launch Account Vending Machine Product | 9 |
| Step 2: Configure User Access | 10 |
| Appendix A: Configuration ZIP File..... | 11 |
| Appendix B: Modifying the solution parameters | 12 |
| AWS CloudTrail..... | 12 |
| AWS Config | 13 |
| AWS Config Rules | 14 |
| AWS IAM Password Policy | 15 |
| AWS Landing Zone Notifications | 16 |
| AWS Landing Zone Security Roles | 17 |

About This Guide

This user guide provides an overview of the AWS Landing Zone solution as well as usage and operation considerations when using the Account Vending Machine(AVM) to create new AWS accounts.

This guide is intended for IT infrastructure architects, administrators, and DevOps professionals who are responsible for using the AWS Landing Zone to create new AWS accounts.

Overview

The AWS Landing Zone solution provides an out-of-the-box multi-account environment as a starting point for implementing a customer's multi-account strategy. This solution can help save customers time by automating the set-up of their environments for running secure and scalable workloads. It also provides customers with a baseline environment that gets them started with a multi-account architecture, identity and access management, governance, data security, network design, and logging.

AWS Landing Zone includes four accounts (AWS Organizations, Shared Services, Logging, and Security), a centralized bucket for storing all AWS CloudTrail logs, cross-account roles for security audit and emergency access, AWS Managed Microsoft Active Directory, AWS CloudFormation StackSets, optional [AWS Service Catalog](#) products, and an Account Vending Machine (AVM) for creating new accounts. This guide describes the AWS Landing Zone multi-account solution and process for using the included AVM to create new, baselined AWS accounts.

Considerations

When you create an account, AWS Organizations initially assigns a password to the root user that is a minimum of 64 characters long. All characters are randomly generated with no guarantees on the appearance of certain character sets. You can't retrieve this initial password. To access the account as the root user for the first time, you must go through the process for password recovery. Consider these best practices when creating an account:

- Follow the Identity and Access Management (IAM) [best practices](#) for securing your AWS resources.
- Don't use the root user to access your account except to create other users and roles with more limited permissions. Sign in as one of those users or roles.

- Set [multi-factor authentication](#) (MFA) on the root user. Reset the password, and then [assign an MFA device to the root user](#).

For more information, see AWS Organizations [Accessing a Member Account as the Root User](#) documentation.

AWS Landing Zone Configuration

The AWS Landing Zone configuration ZIP file contains a manifest file and related templates to create the AWS environment in the following diagram:

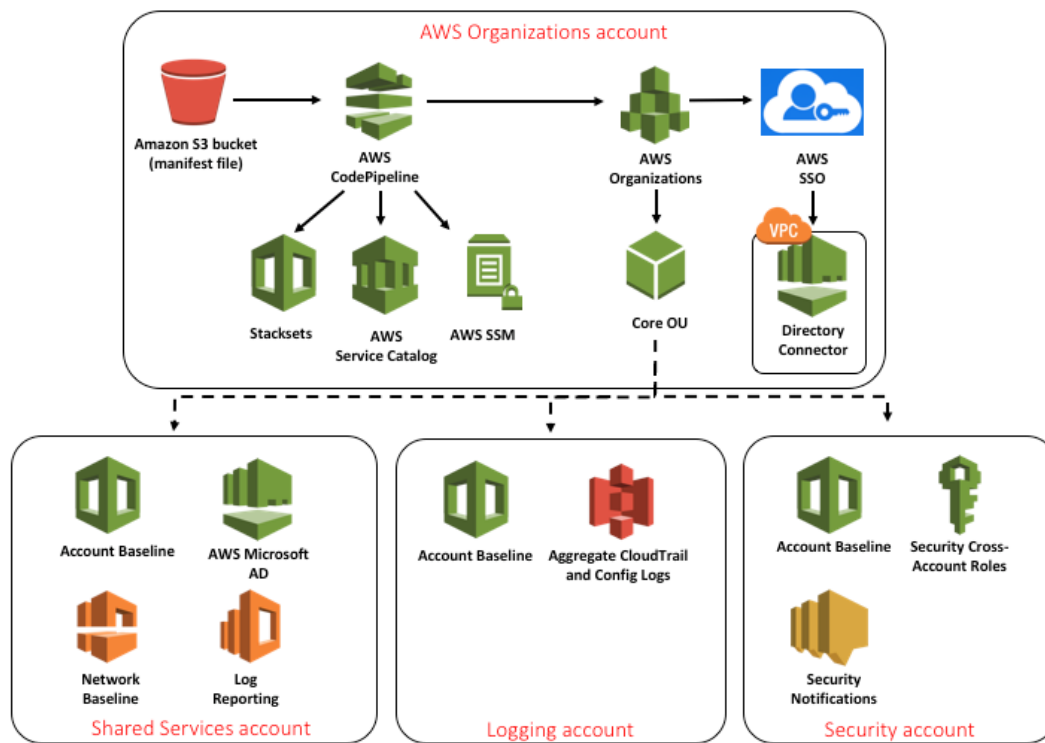


Figure 1: AWS Landing Zone Implementation architecture

AWS Accounts

Organization Account

The AWS Landing Zone is deployed into the [AWS Organization](#) account. This account is used to financially manage accounts, create new accounts, and manage configuration and access to AWS Landing Zone managed accounts. It contains the AWS Landing Zone configuration Amazon Simple Storage Service (Amazon S3) bucket and pipeline, account configuration StackSets, [AWS Organizations Service Control Policies](#) (SCPS), and [AWS Single Sign-On](#)

(SSO) with Directory Connector. For more information about these components, see the [AWS Landing Zone Implementation Guide](#).

Shared Services Account

The Shared Services account is a reference for creating infrastructure shared services like directory services. By default, this account hosts AWS Managed Active Directory for AWS SSO integration in a shared Amazon Virtual Private Cloud (Amazon VPC) that can be automatically peered with new AWS accounts created with the Account Vending Machine (AVM). During AWS Landing Zone installation this VPC is automatically peered with a VPC in the AWS Organizations account to provide network connectivity between Directory Connector and AWS Managed AD.

This account can be used to host additional shared services like log analytics and reporting. For example, an optional centralized logging AWS Service Catalog product is included with AWS Landing Zone to easily deploy an Amazon Elasticsearch and Kibana-base centralized log analysis and reporting solution into your Landing Zone. For more information about enabling this optional component, see [Centralized Logging](#).

Logging Account

The Logging account creates a central Amazon S3 bucket for storing a copy of all AWS CloudTrail and AWS Config log files in a log account. We recommend access to this account be restricted to auditors or security teams for compliance and forensic investigations related to account activity. A second copy of AWS CloudTrail logs for operational use are created locally in each account. For more information, see Security Baseline.

Security Account

The Security account creates auditor (read-only) and administrator (full-access) cross-account roles from a Security account to all AWS Landing Zone managed accounts. The intent of these roles is to be used by a company's security and compliance teams to audit or perform emergency security operations in case of an incident. As a result, we strongly recommend that this account be restricted to authorized security and compliance personnel, and related security or audit tools.

Security Notification Architecture

Two aggregate security notification Amazon Simple Notification Service (Amazon SNS) topics are also created in this account as depicted in the following diagram:

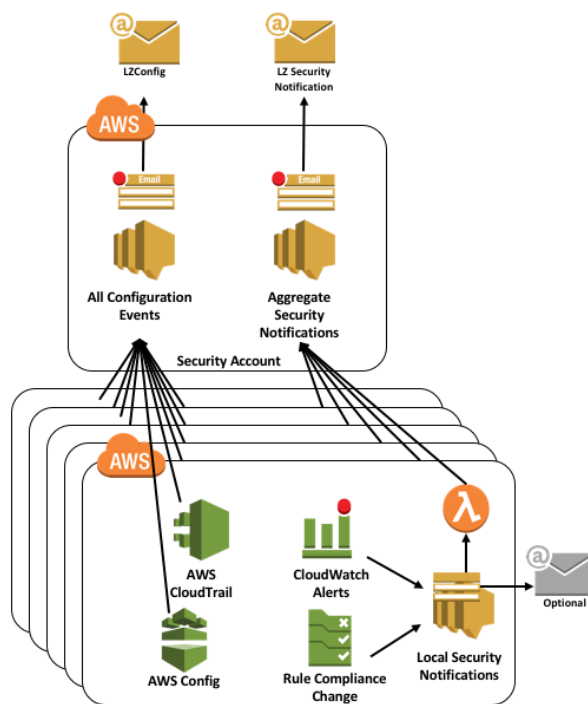


Figure 2: AWS Landing Zone Notifications architecture

The All Configuration Events topic aggregates AWS CloudTrail and AWS Config notifications from all managed accounts. Customers can use this topic for integration with configuration management, change control, or security systems for automatic account change notifications. The second topic aggregates security notifications from specific [Amazon CloudWatch](#) events. Security notifications in each managed account initially send alerts to a local Amazon SNS topic, which leverages an AWS Lambda subscription to forward notifications to the Security account. This architecture is used to allow local administrators to subscribe to specific account notifications, while still aggregating all account notifications to a centralized security account. For more details about security notifications and configurations, see [AWS Landing Zone Notifications](#).

Security Baseline

The AWS Landing Zone solution includes an initial security baseline that can be used as a starting point for establishing and implementing a customized account security baseline for your organization. By default, deploying the AWS Landing Zone solution will deploy this security baseline to the core accounts and to new accounts created with the AVM.

The security baseline is described in the manifest file and related templates in the AWS Landing Zone configuration ZIP file and is deployed through AWS CloudFormation StackSets when new accounts are created by the AVM. By default, the initial security baseline

includes the following settings (for more information about modifying these defaults, see [Appendix B](#): Modifying the solution parameters):

- [AWS CloudTrail](#): One CloudTrail trail is created in each account configured to log to a centrally managed Amazon Simple Storage Service (Amazon S3) bucket in the logging account, and to AWS CloudWatch Logs in the local account for local operations (with a 14-day log group retention policy).
- [AWS Config](#): AWS Config is enabled and account configuration log files are stored in a centrally managed Amazon S3 bucket in the logging account.
- [AWS Config Rules](#): AWS Config rules are enabled for monitoring storage encryption (Amazon Elastic Block Store, Amazon S3, and Amazon Relational Database Service), AWS Identity and Access Management (IAM) password policy, root account multi-factor authentication (MFA), Amazon S3 public read and write, and insecure security group rules.
- [AWS Identity and Access Management](#) (IAM): Configures an IAM password policy with the following settings:
 - Allow users to change their password: true
 - Prevent users from changing expired passwords: false
 - Password complexity: Require uppercase, lowercase, symbols, and numbers
 - Minimum password length: 12
 - Prevent reusing passwords: 6
 - Maximum password age: 90 days
- [Cross-Account Access](#): Configures audit and emergency security administrative access to AWS Landing Zone accounts from the security account.
- [Amazon Virtual Private Cloud](#) (VPC): Configures the initial network for an account. This includes deleting the default VPC in all regions, deploying the AVM requested network type, and network peering with the Shared Services VPC when applicable.
- [AWS Landing Zone Notifications](#): Configures AWS CloudWatch alarms and events to send a notification on root account login, console sign-in failures, API authentication failures, and the following changes within an account to: Security Groups, Network ACLs, Amazon VPC gateways, peering connections, ClassicLink, Amazon Elastic Compute Cloud (Amazon EC2) instance state, large Amazon EC2 instance state, AWS CloudTrail, IAM policies, and AWS Config rule compliance status.

- [\(Optional\) Centralized Logging](#): If enabled, the optional centralized logging component, a Lambda function and cross-account role will be created to allow AWS CloudTrail and other AWS CloudWatch Logs to be stored and indexed in the Amazon Elasticsearch cluster hosted in the Shared Services account.

The default AWS CloudTrail, AWS Config, AWS Config Rules, and IAM password policy settings can be modified by changing the solution input parameter JSON files located in the configuration zip file `parameters/aws_baseline/` directory, reziping (See the [note](#) in Appendix A) the configuration file, and uploading to the AWS Landing Zone configuration Amazon S3 bucket. For more information, see [Appendix A](#).

Account Vending Machine Architecture

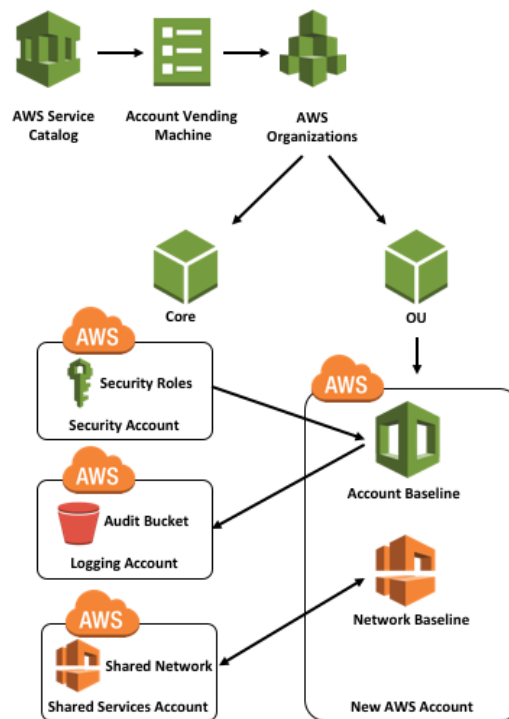


Figure 3: AWS Landing Zone Account Vending Machine architecture

The Account Vending Machine (AVM) is an AWS Landing Zone key component. The AVM is provided as an AWS Service Catalog product, which allows customers to create new AWS accounts in Organizational Units (OUs) preconfigured with an account security baseline, and a predefined network.

AVM Permissions

AWS Landing Zone leverages AWS Service Catalog to grant AWS Service Catalog administrators permissions to create and manage AWS Landing Zone products and end user's permissions to launch and manage AVM products. The AVM uses launch constraints to allow end users to be able to create new accounts without requiring account administrator permissions. For more information about authentication and access control, see the [AWS Service Catalog Administrator Guide](#).

Access to provision new accounts with AVM can be granted directly to end-users or another request management system using [AWS Identity and Access Management](#) (IAM) and [AWS Service Catalog](#) permissions. AWS IAM entities must be granted AWS Service Catalog end-user permissions by either using the `AWSServiceCatalogEndUserFullAccess` AWS managed policy, or a [custom policy](#), to grant access to make AWS Service Catalog API calls. Additionally, IAM principals (users or roles) must be [granted access](#) to the **AWS Landing Zone – Baseline** portfolio in AWS Service Catalog.

Creating New Accounts

Step 1. Launch Account Vending Machine Product

Use the following steps when creating a new vended account:

1. Navigate to the [AWS Service Catalog](#) console.
2. In the **Products List**, select the **AWS-Landing-Zone-Account-Vending-Machine** product.
3. Select **Launch Product**.
4. **Provide** a name for your new account, select the appropriate **AVM version** (the AVM version corresponds with your account configuration baseline version), and select **Next**.
5. Under **Parameters**, review the parameters for the new account and modify them as necessary. The AVM uses the following default values:

| Parameter | Default | Description |
|------------------------|------------------|---|
| Account Name | <Requires input> | Provide a name for the new account. |
| Account Email | <Requires input> | Email address to be used to identify the new account. |
| Organization Unit Name | <Requires input> | A drop-down list of Organizational Units to associate the new account with. This list is managed by the AWS Landing Zone manifest file. |

| Parameter | Default | Description |
|-------------------------------|----------------|--|
| Network Type | No-Primary-VPC | A drop-down list optional Amazon VPC network patterns to create in the account. |
| Network Region | us-east-1 | List of AWS regions for the account's Amazon VPC to be created in. |
| Network CIDR Range | 10.0.0.0/16 | Network CIDR range for the account's Amazon VPC. The AVN will automatically divide this CIDR block into subnets based on the selected network pattern. |
| Peer with Shared-Services VPC | false | Option to peer this account's Primary VPC's Private Subnets with the Shared Service VPC's Private Subnets. |

Step 2: Configure User Access

After creating a new account, use the following steps to configure user access to the new account with AWS SSO:

Optional: Create new Microsoft Active Directory group(s) for managing user access to the new account. For example, a group could be created for each role requiring account access, such as account administrators, power users, read-only users, etc.

1. Navigate to the Dashboard and select **Configure SSO access to your AWS accounts**.
2. Select the new **AWS account** to map Microsoft Active Directory Users or Groups to.
3. Select **Assign Users** and search for the appropriate Group or User Name.
4. Select **Next: Permission sets**.
5. Select **Create New Permission Set**.
6. Select **Use an existing job function policy** and select the appropriate policy.
7. Select the **permission set** and select **Finish**.

Once this process is finished, your users will be able to use the **AWS SSO URL** to access the new account.

Appendix A: Configuration ZIP File

The AWS Landing Zone configuration ZIP file is organized as follows:

| Folder | Description |
|--|--|
| Note: After reziping, please verify the directory structure of the new zipped file matches the following structure. | |
| parameters | Default location for AWS CloudFormation template input parameters |
| parameters/aws_baseline | Parameter files for AWS Landing Zone account baseline templates |
| parameters/core_accounts | Parameter files for AWS Landing Zone core account resource templates |
| parameters/optional_products | Parameter files for AWS Landing Zone AWS Service Catalog optional products |
| policies | Default location for AWS Organizations Service Control Policy files |
| templates | Default location for CloudFormation templates |
| templates/aws_baseline | Parameter files for AWS Landing Zone account baseline templates |
| templates/core_accounts | Parameter files for AWS Landing Zone core account resource templates |
| templates/optional_products | Parameter files for AWS Landing Zone AWS Service Catalog optional products |
| validation | Scripts and manifest schema files for validating the AWS Landing Zone configuration. |
| validation/manifest.schema.yaml | Schema definition for the AWS Landing Zone manifest file. This is used during configuration validation to validate the provided AWS Landing Zone manifest file. |
| validation/run-validation.sh | Validation script for validating the AWS Landing Zone manifest schema and running AWS CloudFormation <code>validate-template</code> and <code>cfn_nag_scan</code> on all AWS CloudFormation templates. |
| manifest.yaml | AWS Landing Zone manifest file used to describe the AWS Landing Zone configuration and related AWS CloudFormation templates. |

Appendix B: Modifying the solution parameters

The default AWS CloudTrail, AWS Config, AWS Config Rules, and AWS Identity and Access Management (IAM) password policy settings can be modified by changing the solution input parameter JSON files located in the configuration zip file `parameters/aws_baseline/` directory, reziping (See the [note](#) in Appendix A) the configuration file, and uploading to the AWS Landing Zone configuration Amazon Simple Storage Service (Amazon S3) bucket. Each setting is as follows:

AWS CloudTrail

| Configuration File | Description |
|---|---|
| <code>parameters/aws_baseline/aws-landing-zone-enable-cloudtrail.json</code> | Provides input parameters for configuring AWS CloudTrail |
| <code>templates/aws_baseline/aws-landing-zone-enable-cloudtrail.template</code> | AWS CloudFormation template for enabling and configuring the AWS CloudTrail baseline in each account. |

The solution configures AWS CloudTrail to send a local operational copy of logs to the `CloudTrail/Landing-Zone-Logs` log group with a retention period of 14 days. A publish log file updates the notifications to a shared Amazon Simple Notification Service (Amazon SNS) topic and stores the log files in a centralized log archive bucket. These settings can be modified by editing the **`aws-landing-zone-enable-cloudtrail.json`** parameter file and changing the default values for any of the following **ParameterKeys**:

| ParameterKey | Default | Description |
|--------------------------------|---|--|
| PublishToTopic | true | Configures AWS CloudTrail log file update messages to publish the AWS SNS topic provided by the <code>SNSTopic</code> parameter key. |
| PublishToCloudWatchLogs | true | Configures AWS CloudTrail to publish logs to the AWS CloudWatch Logs log group with the log retention policy provided by the <code>CloudWatchLogsGroupName</code> and <code>LogsRetentionInDays</code> parameter keys. |
| LogsRetentionInDays | 14 | Number of days to retain AWS CloudWatch logs in the <code>CloudWatchLogsGroupName</code> log group. |
| CloudWatchLogsGroupName | <code>CloudTrail/Landing-Zone-Logs</code> | AWS CloudWatch Logs group name for AWS CloudTrail logs. |
| EnableLogFileValidation | true | Enables or disables AWS CloudTrail log file validation. |
| IncludeGlobalEvents | true | Enables or disables AWS CloudTrail logging global events. |
| MultiRegion | true | Enables or disables AWS CloudTrail in all regions. |

| ParameterKey | Default | Description |
|--------------------|---|--|
| SNSTopic | [\$[alfred_ssm_/org/ primary/sns_topic_arn] | AWS SNS topic to send AWS CloudTrail log file notification messages to. By default, AWS Landing Zone will use the organizations account's shared SNS topic ARN from SSM parameter store. |
| TrailBucket | [\$[alfred_ssm_/org/ member/logging/ bucket_name] | Amazon S3 bucket to store AWS CloudTrail log files. By default, AWS Landing Zone will use the logging account's shared bucket from SSM parameter store. |

AWS Config

| Configuration File | Description |
|---|---|
| parameters/aws_baseline/aws-landing-zone-enable-config.json | Provides input parameters for configuring AWS Config |
| templates/aws_baseline/aws-landing-zone-enable-config.template | AWS CloudFormation template for enabling and configuring the AWS Config baseline in each account. |

The solution configures AWS Config to publish configuration update notifications to a shared Amazon SNS topic and stores log files in a centralized log archive bucket. These settings can be modified by editing the **aws-landing-zone-enable-config.json** parameter file and changing the default values for any of the following **ParameterKeys**:

| ParameterKey | Default | Description |
|-----------------------------------|---|--|
| AllSupported | true | Configures AWS Config to track all supported resource type configuration changes. |
| IncludeGlobalResourceTypes | true | Configures AWS Config to include global resource types. |
| ResourceTypes | AWS::CloudTrail::Trail | Optional resource types to use if parameter AllSupported is disabled (false). |
| DeliveryChannelName | Landing-Zone-Delivery-Channel | AWS Config delivery channel name. |
| Frequency | 24hours | The frequency with which AWS Config delivers configuration snapshots. |
| TopicArn | [\$[alfred_ssm_/org/ primary/sns_topic_arn] | Amazon SNS topic to send AWS Config notification messages to. By default, AWS Landing Zone will use the organizations account's shared SNS topic ARN from SSM parameter store. |
| BucketName | [\$[alfred_ssm_/org/ member/logging/ bucket_name] | Amazon S3 bucket to store AWS Config log files. By default, AWS Landing Zone will use the logging account's shared bucket from SSM parameter store. |

AWS Config Rules

| Configuration File | Description |
|---|---|
| parameters/aws_baseline/aws-landing-zone-enable-config-rules.json | Provides input parameters for configuring AWS Config Rules. |
| templates/aws_baseline/aws-landing-zone-enable-config-rules.template | AWS CloudFormation template for enabling and configuring the AWS Config Rules baseline in each account. |

The solution provides seven out-of-the-box AWS Config Rules that can be modified by editing the **aws-landing-zone-enable-config-rules.json** parameter file and changing the default values for any of the following **ParameterKeys**:

| ParameterKey | Default | Description |
|---|---------|--|
| EnableEncryptedVolumesRule | true | Enables the AWS managed encrypted-volumes config rule. To disable, change the parameter value to false. |
| EnableRdsEncryptionRule | true | Enables the AWS managed rds-storage-encrypted config rule. To disable, change the parameter value to false. |
| EnableS3PublicReadRule | true | Enables the AWS managed s3-bucket-public-read-prohibited config rule. To disable, change the parameter value to false. |
| EnableS3PublicWriteRule | true | Enables the AWS managed s3-bucket-public-write-prohibited config rule. To disable, change the parameter value to false. |
| EnableS3ServerSideEncryptionRule | true | Enables the AWS managed s3-bucket-server-side-encryption-enabled config rule. To disable, change the parameter value to false. |
| EnableRootMfaRule | true | Enables the AWS managed root-account-mfa-enabled config rule. To disable, change the parameter value to false. |
| EnableIamPasswordPolicyRule | true | Enables the AWS managed iam-password-policy config rule. To disable, change the parameter value to false. |
| EnableRestrictedCommonPortsRule | true | Enables the AWS managed restricted-common-ports config rule. To disable, change the parameter value to false. |
| EnableRestrictedSshRule | true | Enables the AWS managed restricted-ssh config rule. To disable, change the parameter value to false. |
| KMSId | <blank> | Optional KMS key ID to use as part of the encrypted-volumes of rds-storage-encrypted rules. |

| ParameterKey | Default | Description |
|-----------------------------------|------------------|--|
| MaximumExecutionFrequency | TwentyFour_Hours | Configures the frequency for root-account-mfa-enabled and iam-password-policy config rule execution. |
| RequireUppercaseCharacters | true | IAM password complexity requirement check for iam-password-policy config rule. |
| RequireLowercaseCharacters | true | IAM password complexity requirement check for iam-password-policy config rule. |
| RequireSymbols | true | IAM password complexity requirement check for iam-password-policy config rule. |
| RequireNumbers | true | IAM password complexity requirement check for iam-password-policy config rule. |
| MinimumPasswordLength | 12 | IAM password complexity requirement check for iam-password-policy config rule. |
| PasswordReusePrevention | 6 | IAM password reuse policy check for iam-password-policy config rule. |
| MaxPasswordAge | 90 | IAM password maximum age policy check for iam-password-policy config rule. |

AWS IAM Password Policy

| Configuration File | Description |
|---|--|
| parameters/aws_baseline/aws-landing-zone-iam-password-policy.json | Provides input parameters for configuring the AWS IAM password policy. |
| templates/aws_baseline/aws-landing-zone-iam-password-policy.template | AWS CloudFormation template for enabling and configuring the AWS IAM password policy baseline in each account. |

The solution configures an account's IAM password policy that can be modified by editing the **aws-landing-zone-iam-password-policy.json** parameter file and changing the default values for any of the following **ParameterKeys**:

| ParameterKey | Default | Description |
|-----------------------------------|---------|---|
| AllowUsersToChangePassword | true | Configures whether or not IAM will allow users to change their own password. |
| HardExpiry | false | Configures whether or not IAM will allow users to change their password after it has expired. |
| RequireUppercaseCharacters | true | IAM password complexity requirement check for iam-password-policy config rule. |
| RequireLowercaseCharacters | true | IAM password complexity requirement check for iam-password-policy config rule. |

| ParameterKey | Default | Description |
|--------------------------------|---------|--|
| RequireSymbols | true | IAM password complexity requirement check for iam-password-policy config rule. |
| RequireNumbers | true | IAM password complexity requirement check for iam-password-policy config rule. |
| MinimumPasswordLength | 12 | IAM password complexity requirement check for iam-password-policy config rule. |
| PasswordReusePrevention | 6 | IAM password reuse policy check for iam-password-policy config rule. |
| MaxPasswordAge | 90 | IAM password maximum age policy check for iam-password-policy config rule. |
| LogsRetentionInDays | 14 | Number of days to retain the AWS CloudFormation custom resource log files generated by AWS Lambda when implementing this IAM password policy baseline. |

AWS Landing Zone Notifications

| Configuration File | Description |
|---|--|
| parameters/aws_baseline/aws-landing-zone-notifications.json | Provides input parameters for configuring AWS Landing Zone notifications to be sent to the notification email from each account. |
| templates/aws_baseline/aws-landing-zone-notifications.template | AWS CloudFormation template for enabling and configuring AWS Landing Zone notifications in each account. |

The solution configures each account to send notifications to a local Amazon SNS topic (`AWS-Landing-Zone-Security-Notifications`). An AWS Lambda function is automatically subscribed to this topic to forward all notifications to an aggregation Amazon SNS topic in the AWS Organizations account (`AWS-Landing-Zone-Aggregate-Security-Notifications`). This architecture is designed to allow local operators to subscribe to receive account-specific security notifications, while also providing the ability to received aggregate notifications centrally.

The specific security notifications can be modified by editing the **aws-landing-zone-notifications.json** parameter files and changing the default values for any of the following **ParameterKeys**:

| ParameterKey | Default | Description |
|----------------------------|------------------------------|---|
| LogGroupName | CloudTrail/Landing-Zone-Logs | AWS CloudWatch log group for AWS CloudTrail events to monitor. |
| LogsRetentionInDays | 14 | Number of days to retain logs for the notification AWS Lambda function. |

| ParameterKey | Default | Description |
|--|---|---|
| AlarmNotificationTopic | [\$[alfred_ssm_/org/primary/sns_notification_arn] | Amazon SNS topic to send security notification messages to. By default, AWS Landing Zone will use the organizations account's shared notification SNS topic ARN from SSM parameter store. |
| NotifyDisplayName | LZNotify | Amazon SNS topic display name for the account's notification topic. |
| NotifyTopicName | AWS-Landing-Zone-Security-Notifications | Amazon SNS topic name for the account's notification topic. |
| EnableSecurityGroupChangeAlarm | true | Send a notification if Amazon EC2 or Amazon VPC security groups are changed. |
| EnableNetworkAclChangeAlarm | true | Send a notification if Amazon VPC network access control lists (ACLs) are changed. |
| EnableGatewayChangeAlarm | true | Send a notification if Amazon VPC internet or customer gateways are changed. |
| EnableVpcChangeAlarm | true | Send a notification if Amazon VPCs are created or deleted, or if VPC peering or ClassicLink connections are changed. |
| EnableEc2InstanceChangeAlarm | true | Send a notification on any Amazon EC2 instance status changes. |
| EnableEc2LargeInstanceChangeAlarm | true | Send a notification on Amazon EC2 instance status changes for 4x, 8x, 9x, 10x, 12x, 16x, 18x, 24x, 32x-large instance sizes. |
| EnableCloudTrailChangeAlarm | true | Send a notification on AWS CloudTrail changes. |
| EnableConsoleSignInFailureAlarm | true | Send a notification on 3 console sign-in failures within 5 minutes of each other. |
| EnableAuthorizationFailureAlarm | true | Send a notification on any AWS API authorization failure. |
| EnableIamPolicyChangesAlarm | true | Send a notification on IAM policies changes. |
| EnableRootLoginAlarm | true | Send a notification on root user login. |
| EnableConfigRuleComplianceChangeAlarm | true | Send a notification whenever the compliance status of an AWS Config rule changes. |

AWS Landing Zone Security Roles

| Configuration File | Description |
|--|---|
| parameters/core_accounts/aws-landing-zone-security.json | Provides input parameters for configuring the AWS Landing Zone security account cross-account role names. |

| Configuration File | Description |
|--|--|
| parameters/aws_baseline/aws-landing-zone-security-roles.json | Provides input parameters for configuring the AWS Landing Zone cross-account security roles in each account. |
| templates/aws_baseline/aws-landing-zone-security-roles.template | AWS CloudFormation template for enabling and configuring the AWS Landing Zone security baseline roles in each account. |

The solution configures each account with administrator and read-only cross-account roles from a security account. This configuration can be modified by editing the **aws-landing-zone-security.json** and **aws-landing-zone-security-roles.json** parameter files and changing the default values for any of the following **ParameterKeys**:

| ParameterKey | Default | Description |
|---------------------------------------|--|---|
| EnableAdminRole | true | Configures whether or not to enable an administrator cross-account role. |
| EnableReadOnlyRole | true | Configures whether or not to enable a read-only cross-account role. |
| AdminRoleName | AWSLandingZoneAdminExecutionRole | The name of the IAM admin role to create in each account that will allow cross-account access from the security account. |
| ReadOnlyRoleName | AWSLandingZoneReadOnlyExecutionRole | The name of the IAM read-only role to create in each account that will allow cross-account access from the security account. |
| SecurityAccountAdminRoleArn | [\$[alfred_ssm_/org/member/security/admin_role_arn] | The role ARN for enabling cross-account access. By default, AWS Landing Zone will use the security account's admin role ARN from SSM parameter store. |
| SecurityAccountReadOnlyRoleArn | [\$[alfred_ssm_/org/member/security/readonly_role_arn] | The role ARN for enabling cross-account access. By default, AWS Landing Zone will use the security account's read-only role ARN from SSM parameter store. |

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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/>.