AWS Landing Zone

AWS User Guide

November 2018

Contents

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, Log Archive, and Security, a centralized bucket for storing all AWS CloudTrail logs, cross-account roles for security audit and emergency access, AWS CloudFormation StackSets, optional AWS Service Catalog add-on products, and an Account Vending Machine (AVM) for creating and baselining 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:

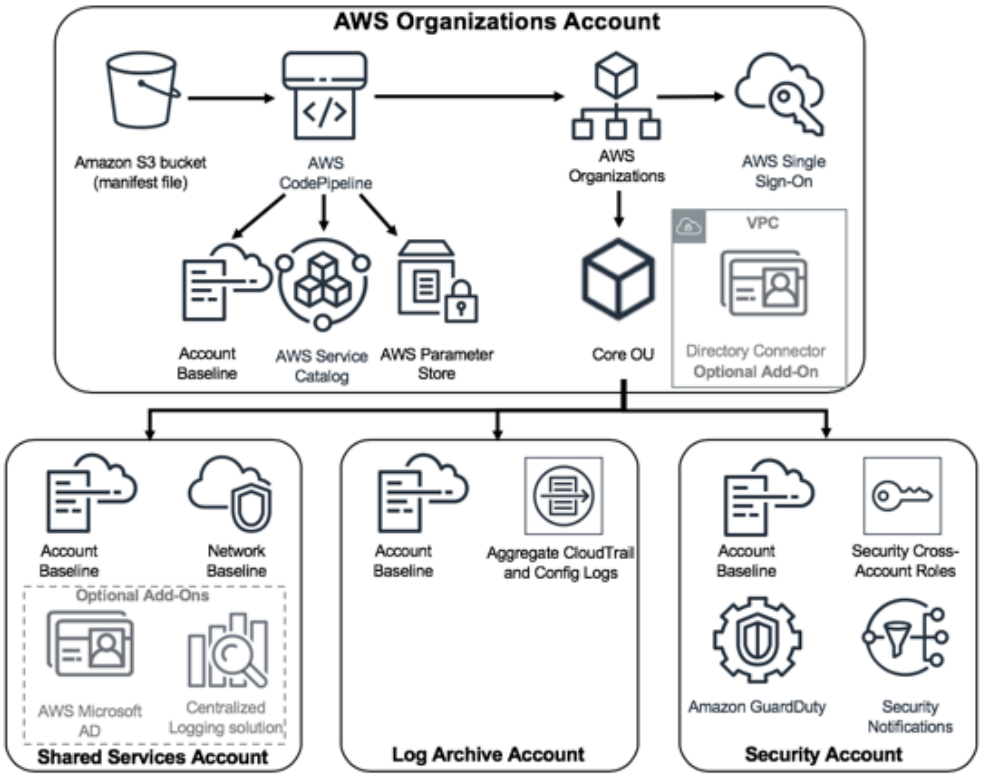


Figure 1: AWS Landing Zone Implementation architecture

AWS Accounts

Organization Account

The AWS Landing Zone is deployed into the AWS Organizations 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). 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 such as directory services. By default, this account hosts an Amazon Virtual Private Cloud (Amazon VPC) that can be automatically peered with new AWS accounts created with the Account Vending Machine (AVM).

This account can be used to host additional shared services such as AWS Managed Active Directory for AWS SSO integration, log analytics and reporting. For example, an optional centralized logging AWS Service Catalog add-on 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.

Log Archive Account

The Log Archive 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 security and compliance teams to audit, such as hosting custom AWS Config Rule lambda functions, or perform automated security operations, such as perform remediation actions. As a result, we strongly recommend that this account be restricted to authorized security and compliance personnel, and related security or audit tools.

The Security account is also designated as the **master** Amazon GuardDuty account. Users from the master account can configure GuardDuty as well as view and manage GuardDuty findings for their own account and all of their **member** accounts. Members are invited and associated to the **master** account as part of the Security Baseline.

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:

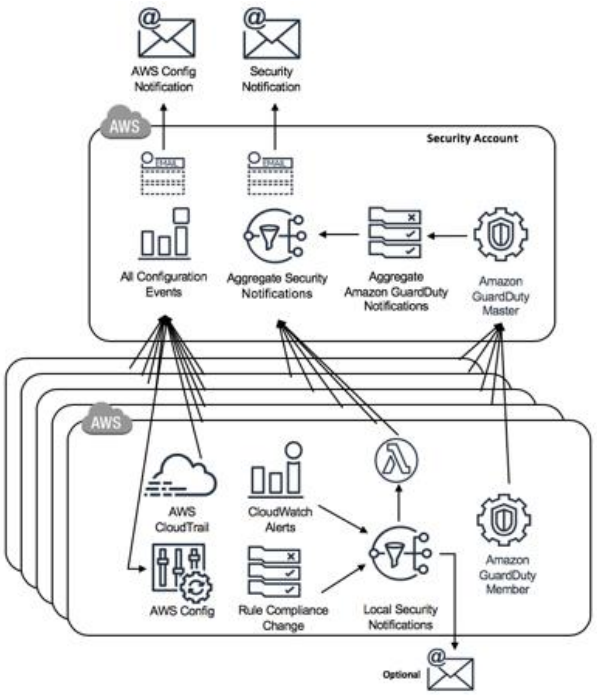


Figure 2: AWS Landing Zone Notifications architecture

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 **Aggregate Security Notifications** topic aggregates security notifications from specific Amazon CloudWatch events, AWS Config Rules compliance status change events, and AWS GuardDuty findings. Security notifications in each managed account sends alerts to a local Amazon SNS topic, an AWS Lambda function sends 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 A:

- AWS CloudTrail: One CloudTrail trail is created in each account and configured to send logs to a centrally managed Amazon Simple Storage Service (Amazon S3) bucket in the log archive 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 log archive 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 Amazon 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.
- Amazon GuardDuty Member: Amazon GuardDuty **member** is created and associated with the Amazon GuardDuty **master**. Generated findings and activity in the member account can be viewed and managed by allowed users in the member account, and from the Amazon GuardDuty master 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. For more information, see Appendix B.

Account Vending Machine Architecture

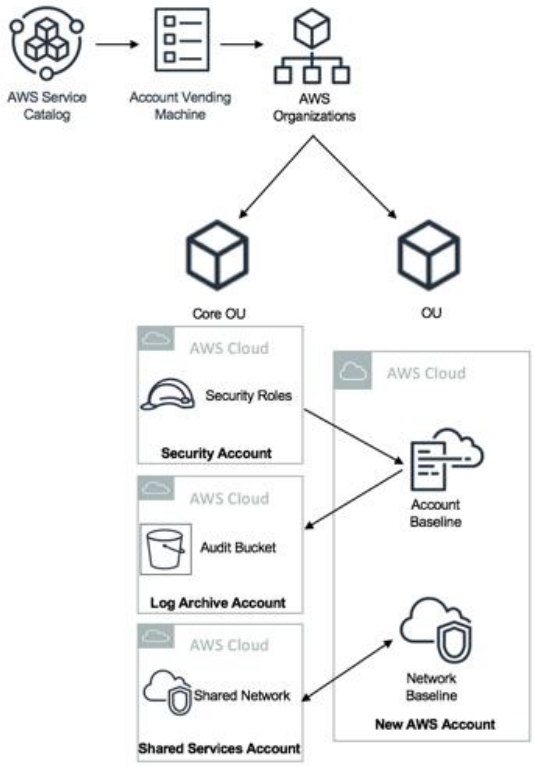


Figure 3: AWS Landing Zone Account Vending Machine architecture

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 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 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 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** and **AWS Landing Zone – Add-On Products** portfolio in the AWS Service Catal

Also need AmazonSNSFullAccess to be able to create the topic for provisioned account notifications

Creating New Accounts

The AWS Landing Zone solution lets users create new accounts by deploying AVM through Service Catalog.

Step 1. Launch Account Vending Machine Product

To deploy the Account Vending Machine (AVM), access to the AVM on the Service Catalog's Products list must be enabled. Use the following procedure enable access:

1. In the Organizations master account, 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.
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 AVM will automatically divide this CIDR block into subnets based on the selected network pattern.

AWS Landing Zone Add-On Products

The AWS Service Catalog Portfolio has add-on feature that allow customers to extend their Landing Zone implementation by dropping in the add-on Micro-configuration into their existing Landing Zone Configuration. The default implementation creates the AWS Service Catalog Portfolio **AWS Landing Zone - Add-On Products**, and deploys add-on products.

AWS Managed AD and Directory Connector for AWS SSO

AWS Microsoft Active Directory

This add-on deploys AWS Microsoft Active Directory (Microsoft AD) to provide AWS Single Sign-On (AWS SSO) access to your user directory. By default, Microsoft AD is deployed into the **Shared Services** account to separate AD user management from AWS Landing Zone management functions. This makes it easier to leverage AD for applications or operating system management.

AWS Single Sign-On (AWS 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 lays the foundation for using AWS SSO for managing user access to your AWS accounts. Deploying the add-on sets up AWS Active Directory Connector (AD Connector) in the AWS Organizations account to connect SSO to the Microsoft AD environment for user management in the Shared Services account. After deploying the AWS Landing Zone initialization template, Configure AWS SSO provides detailed instructions for enabling and integrating AWS SSO into your Landing Zone. The following diagram depicts the AWS SSO implementation:

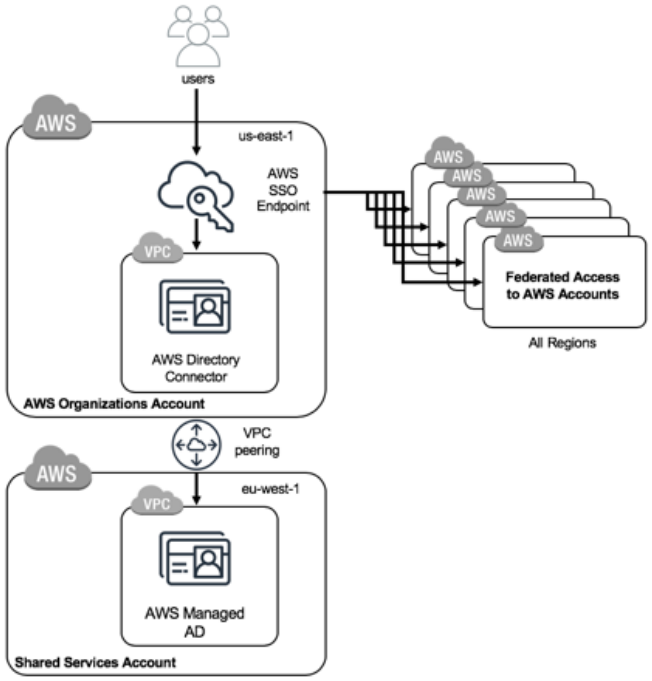


Figure 4: AWS Landing Zone AWS SSO architecture on AWS

AWS SSO Endpoint

AWS SSO creates a single-sign-on endpoint to federate user access to AWS accounts. Currently, AWS SSO endpoints can only be created in US East (N. Virginia), however, this endpoint can be used to federate access into any AWS account in any region.

Active Directory Connector

AD Connector is a directory gateway for redirecting directory requests to Microsoft AD running on-premises or in another AWS account. The solution leverages AD Connector to connect AWS SSO in the AWS Organizations account to a Microsoft AD environment for user management. The implementation integrates AD Connector with AWS Directory Service running in a shared services account using an Amazon Virtual Private Cloud (Amazon VPC) peering connection.

The architecture can be modified to support alternative AD implementations:

- AD Connector can be configured to point directly to an existing AD environment using a VPC peering, VPN, or Direct Connect connection. For more information, see Active Directory Connector.

- AD Connector can be replaced with AWS Directory Service in the AWS Organizations account for establishing advanced AD trust relationships with existing AD environments using a VPC peering, VPN, or Direct Connect connection.

Step 1: Launch Product

Use the following steps to launch the AWS Active Directory add-on product:

Note: This add-on product must be deployed as a pre-requisite.

1. Navigate to the **AWS Service Catalog** console, in the **Products List**, select the **AWS Managed AD and Directory Connector for AWS SSO** - Landing Zone Add-On product
2. Select **Launch Product**.
3. **Provide** a name for your new add-on, select the appropriate **version**, and select **Next**.
4. Under **Parameters**, review the parameters for the new account and modify them as necessary. This add-on product uses the following default values:

Account/Region Selection		
Parameter	**Default**	**Description**
Core Account Name	shared-services	Provide a name for the existing account where Shared-Services VPC exists.
Master Account Name	primary	Provide a name for the Organizations master account.
Organizational Unit Name	core	A drop-down list of Organizational Units to associate the new account with. This list is managed by the AWS Landing Zone manifest file.
AWS Managed AD Region	*<Requires input>*	Specify the AWS Region where Shared-services VPC exists.
Region	us-east-1	List of AWS Regions the AD Connector VPC will be created in.

Landing Zone Pipeline Configuration		
Parameter	**Default**	**Description**
Auto Deploy Add-On	Yes	Determines if the LZ pipeline starts the add-on zip file is added to the master configuration zip file. Select **No**, if the CodePipeline source has been modified in AWS CodeCommit and requires manual intervention.
Domain DNS Name	example.com	Fully qualified domain name of the forest root domain.

Landing Zone Pipeline Configuration		
Domain Net BIOS Name	example	NetBIOS name of the for users of earlier versions of Windows. **Note:** Cannot be longer than 15 characters.
Password Never Expires	Yes	Option to never allow password expiration for Active Directory admin & connector users.
RDGW Instance Type	t2.micro	Choose the Amazon EC2 instance type for the Remote Desktop Gateway instances.
Allowed Remote Desktop External Access CIDR	*<Requires input>*	Allowed CIDR Block for external access to the Remote Desktop Gateways.
Number of RDGW Hosts	1	Enter the number of Remote Desktop Gateway hosts to create.

AWS SSO Network Configuration		
Parameter	Default	Description
Directory Connect VPC CIDR	10.249.0.0/24	CIDR block for Directory Connect to use for connecting AWS SSO to Active Directory.
Directory Connect VPC Subnet 1	10.249.0.0/27	CIDR block for the Directory Connect VPC subnet created in AZ1
Directory Connect VPC Subnet 2	10.249.0.32/27	CIDR block for the Directory Connect VPC subnet created in AZ2
VPC Flow Logs Retention in Days	90	Specifies the number of days you want to retain VPC flow logs in each account.

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, and read-only users.

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**.

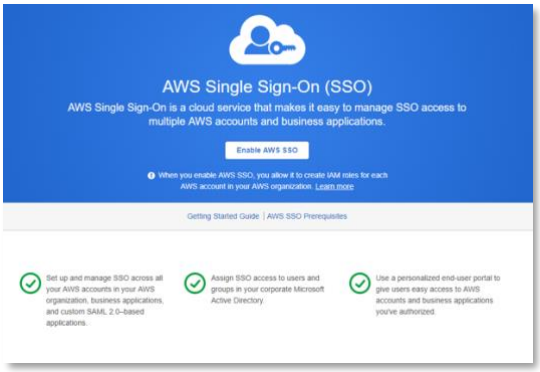
Once completed, users will be able to use the **AWS SSO URL** to access the new account.

Step 3: Create AD user and groups

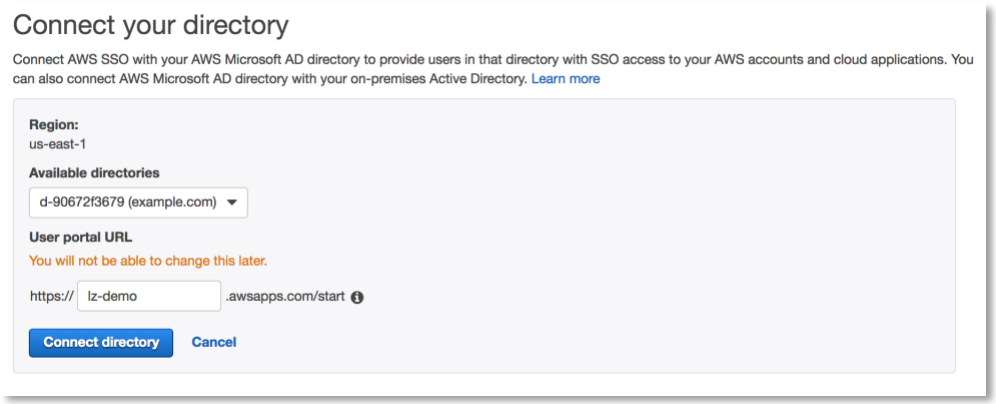
1. Navigate to the **AWS Systems Manager** console, and select the **Parameter Store**.
2. Find the Elastic IP address for a Remote Desktop Gateway (RDGW) stored in the following parameter: `/org/member/sharedservices/rdgw_ip1`
3. Find the AD domain admin username stored in the following parameter: `/org/directory_service/domain_admin_user`
4. Find the AD domain admin password stored in the following parameter: `/org/directory_service/domain_admin_password`
5. Remote desktop into the RDGW using the IP, user name, and password.
6. Launch the **Active Directory Users and Computers** using the following procedure: Select Windows Menu , select Windows Administrative Tools , and select Active Directory Users and Computers.
7. Create groups for access to your core accounts:
    - AWS-Shared-Services-Admins
    - AWS-Shared-Services-Read-Only
    - AWS-Security-Admins
    - AWS-Security-Read-Only
    - AWS-Logging-Admins
    - AWS-Logging-Read-Only
8. Create an **AWS SSO** user, and add the user to the appropriate group(s).

Step 4: Configure AWS SSO

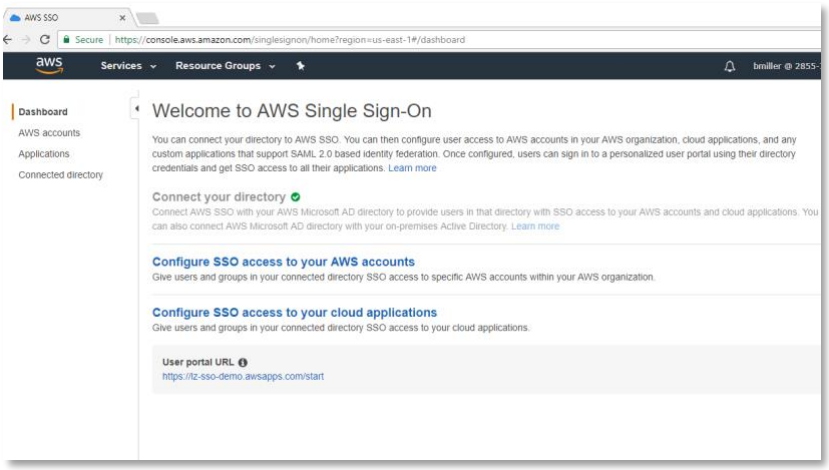
1. Navigate to the **AWS SSO console**, and select **Enable SSO**.



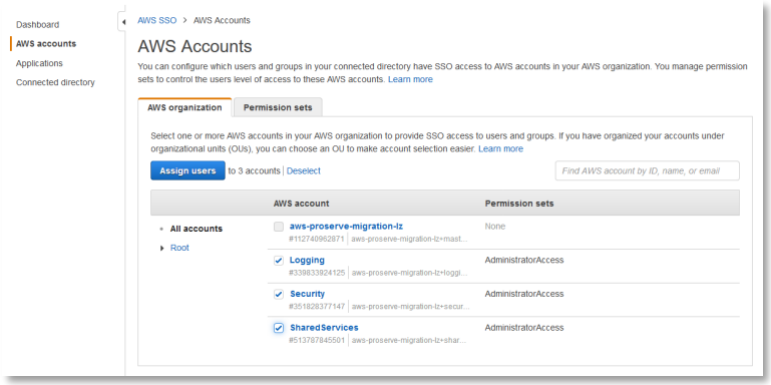
2. Select **Connect your directory**.
3. Select the AWS Landing Zone created directory from **Available directories**, provide a **User portal URL**, and select **Connect directory**.



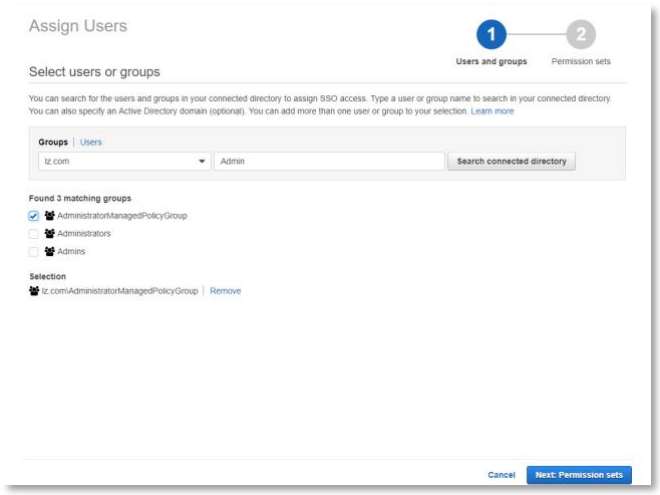
4. Navigate to the Dashboard, and select **Configure SSO access to your AWS accounts**.



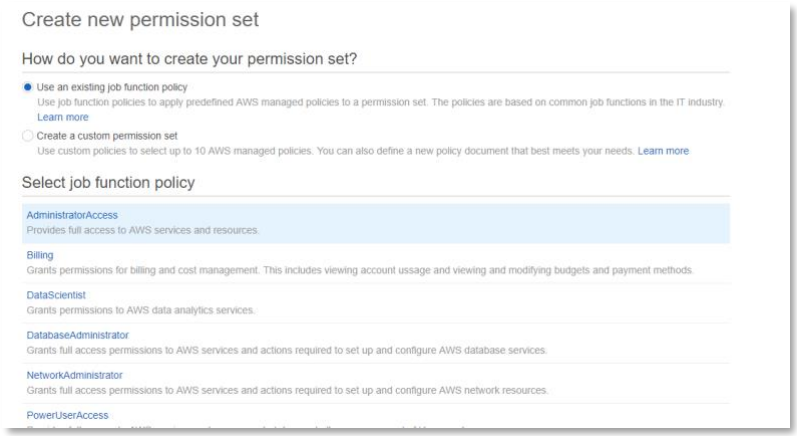
5. Select the **AWS accounts** to map Groups/Users to.



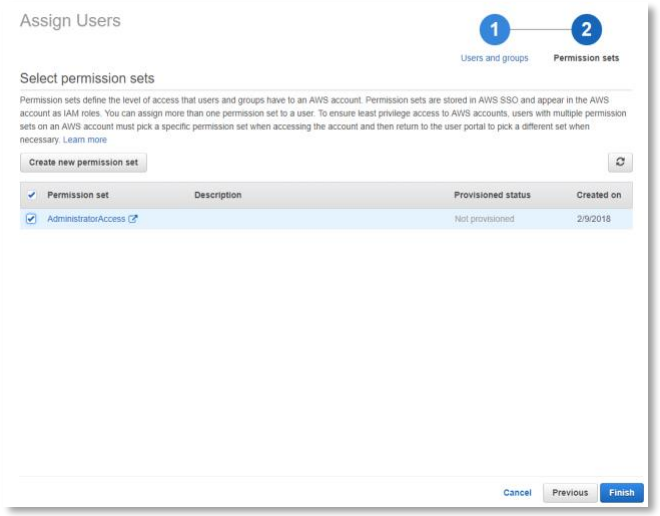
6. Select **Assign Users** and search or enter the Group/User Name.
7. Select **Next: Permission sets**.



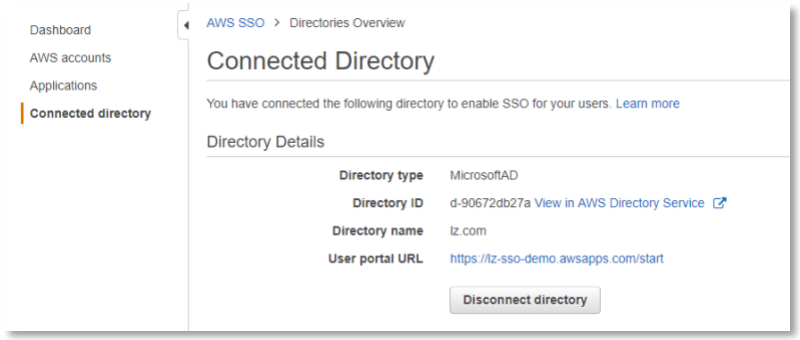
8. Select **Create New Permission set**.
9. Select **Use an existing job function policy**, and select the appropriate policy.



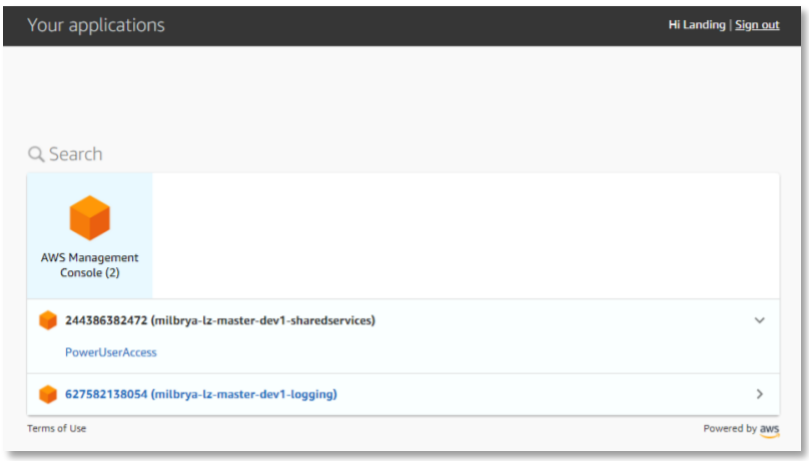
10. Select the **permission set**, and select **Finish**.



Once the process is finished, you can look at the Connected Directory to find the **AWS SSO URL**.



11. Log in to the user portal to access all the assigned AWS accounts and applications.



Launch Centralized Logging Solution Add-On Product

If enabled, the optional centralized logging component, an AWS 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.

Use the following procedure to launch the Centralized Logging Solution add-on product:

1. Navigate to the **AWS Service Catalog** console, in the **Products List**, select the **AWS Centralized Logging Solution -** Landing Zone Add-On product.
2. Select **Launch Product**.
3. **Provide** a name for the new add-on, select the appropriate **version**, and select **Next**.
4. Under **Parameters**, review the parameters for the new account and modify them as necessary. This add-on product uses the following default values:

Account/Region Selection		
Parameter	**Default**	**Description**
Account Name	Shared-services	Provide a name for the new account.
Organizational Unit Name	core	A drop-down list of Organizational Units to associate the new account with. This list is managed by the AWS Landing Zone manifest file.
Centralized Logging Hub Region	us-east-1	List the AWS Region the Centralized Logging Hub will be created in.
Baseline Product Name	AWS-Landing-Zone-Account-Vending-Machine	Name of the existing baseline product in the manifest zip file.
Landing Zone Pipeline Configuration		
Parameter	**Default**	**Description**
Auto Deploy Add-On	Yes	Determines if the LZ pipeline starts after the add-on zip file is added to the master configuration zip file. Select **No**, if the CodePipeline source has been modified in AWS CodeCommit and requires manual intervention.

Centralized Logging Solution Configuration		
Parameter	**Default**	**Description**
Elasticsearch Domain Name	centralizedlogging	Name for the Amazon ES domain that this template will create. Domain names must start with a lowercase letter and must be between 3 and 28 characters. Valid characters are a-z (lowercase only), 0-9.

Centralized Logging Solution Configuration		
Elasticsearch Notification Address	*<Requires input>*	An email address to send Amazon Elasticsearch service CloudWatch alarm notifications
Elasticsearch Cluster Size	Small	Amazon ES cluster size; Small (2 data nodes), Medium (4 data nodes), Large (10 data nodes)
Cognito user email address	*<Requires input>*	Email address to create a Cognito user to access Kibana dashboard.
Centralized Logging Spoke Regions	*<Requires input>*	List of AWS Regions where the Centralized Logging Spoke template will be deployed as a part of the baseline resource. Example: us-east-1, us-east-2

Appendix A: Master Configuration ZIP File

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

> **Note:** After rezipping, verify the directory structure of the new zipped file matches the following structure:

Folder	Description
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
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
template_constraints	Rules files for AWS Service Catalog portfolios created by AWS Landing Zone
manifest.yaml	AWS Landing Zone manifest file used to describe the AWS Landing Zone configuration and related AWS CloudFormation templates.

Use the following commands to unzip, modify, and rezip your configuration file:

```
> unzip aws-landing-zone-configuration.zip -d aws-landing-zone-
configuration
> cd aws-landing-zone-configuration
> # make modifications
> zip -r ../aws-landing-zone-configuration.zip *
```

Add-On Configuration Zip File

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

Note: Creating folders is optional. The folder structure must match the file path provided in the **`add_on_manifest.yaml`** file.

Folder	Description
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
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
template_constraints	Rules files for AWS Service Catalog portfolios created by AWS Landing Zone
user-input.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.
add_on_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, rezipping 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
parameters/aws_baseline/aws-landing-zone-enable-cloudtrail.json	Provides input parameters for configuring AWS CloudTrail
templates/aws_baseline/aws-landing-zone-enable-cloudtrail.template	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 SNSTopic 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 CloudWatchLogsGroupName and LogsRetentionInDays parameter keys.
LogsRetentionInDays	14	Number of days to retain AWS CloudWatch logs in the CloudWatchLogsGroupName log group.
CloudWatchLogsGroupName	CloudTrail/Landing-Zone-Logs	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 log archive 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. 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. 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.
AlarmNotificationTopic	$[alfred_ssm_/org/	Amazon SNS topic to send security notification messages to. By default, AWS Landing Zone

ParameterKey	Default	Description
	primary/sns_notification_arn]	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.
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.

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/.