Landing Zone Immersion Day

Lab 1 – Deploy the Landing Zone

June 2018

Rev 2018-06-18

Table of Contents

Overview

This lab will walk you through the deployment of the **Landing Zone.**

An 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 kicks off the pipeline to build out the landing zone implementation.

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 an AWS Landing Zone Configuration Pipeline and run the solution through the pipeline.

The AWS Landing Zone initialization template provides customers who don't want the three accounts to be created, or would like to modify the solutions core resources, such as Microsoft Active Directory and Directory Connect, before it's run through the pipeline, with the following two options:

- **Auto Build Landing Zone:** This input parameter controls whether or not 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.

- Changing the parameter **Auto Build Landing Zone** 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.

Deploy the Landing Zone Landing Zone

In this section we deploy the Landing Zone Landing Zone Implementation & Configuration Pipeline by means of a **Cloudformation** template.

1. **View the template** – familiarize yourself with the contents of the template by downloading it from here: https://s3.amazonaws.com/solutions-reference/aws-landing-zone/latest/aws-landing-zone-initiation.template
2. Log in to the AWS Management Console for the account you plan on deploying the Landing Zone in to.
3. **Launch the Stack** – click on the following link to launch the Stack.
4. 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]

5. Click **Next**.
6. On the **Specify Details** page, assign a name to your solution stack.
7. 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 Make sure all the email addresses in this template are unique i.e. DO NOT repeat the same email address for any parameter inputs.
Logging Account Email Address	*<Requires input>*	Email address used create a centralized audit log account. Make sure all the email addresses in this template are unique i.e. DO NOT repeat the same email address for any parameter inputs.
Security Account Email Address	*<Requires input>*	Email address used create a centralized security account. Make sure all the email addresses in this template are unique i.e. DO NOT repeat the same email address for any parameter inputs.
Core OU Name	core	Name of Organizations Unit for the Core Accounts.

[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		
Non-Core OU Names	applications	Comma separated list of additional Organizations Unit names for organizing additional AWS accounts by applications, business units, etc.
Security Alert Email Address	*<Requires input>*	Email for all the Security Alerts related to Landing Zone. Make sure all the email addresses in this template are unique i.e. DO NOT repeat the same email address for any parameter inputs.
Lock StackSets ExecutionRole	No	Locks down the AWS StackSets Execution role in the member accounts to only allow access from provisioning roles. (I.E. It locks down the account to only the required lambda and StackSetAdmin roles from the master account can access child accounts)
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	<blank>	Optional email address to subscribe to all change events if "Subscribe All Change Events Email to Topic" is 'Yes"

8. Set the Pipeline Approval Stage to **Yes** if you prefer to have an approval step for modifications to the Landing Zone itself.
9. Ensure you set the **Auto Build Landing Zone** setting to **Yes**.

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>*	(Not required if Pipeline Approval Stage = 'No') Email for notifying that the Landing Zone pipeline is waiting for an Approval. Make sure all the email addresses in this template are unique i.e. DO NOT repeat the same email address for any parameter inputs.
Auto Build Landing Zone	Yes	Do you want to trigger the pipeline right away to build the Landing Zone?

10. Choose the region for your Active Directory Deployment.

Active Directory Configuration		
Parameter	**Default**	**Description**
AD Region	*<Requires input>*	Region for AD to be deployed into. This will likely be the same region you've currently selected.

Active Directory Configuration		
Shared Service 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 Microsfot AD. You can modify the address range to avoid overlapping with existing networks.
Domain DNS Name	example.com	Fully qualified domain name of the forest root domain
Domain Net BIOS Name	example	NetBIOS name of the for users of earlier versions of Windows. **Note:** Cannot be longer than 15 characters.
RDGW Instance Type	t2.large	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. If you're on Amazon network, click here to find your current IP, if you're on Internet outside of Amazon, click here to find your current IP
Number of RDGW Hosts	1	Enter the number of Remote Desktop Gateway hosts to create

AWS SSO Network Configuration		
Parameter	**Default**	**Description**
AWS SSO region endpoint	us-east-1	List of AWS SSO supported endpoint regions.
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 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.

AWS Config Rules		
Parameter	**Default**	**Description**

AWS Config Rules		
Enable Encrypted Volume Rule	Yes	Enable EBS encrypted volume Config Rule?
Enable RDS Encryption Rule	Yes	Enable RDS encrypted volume Config Rule?
Enable S3 Public Read Rule	Yes	Enable check for S3 buckets with public read enabled Config Rule?
Enable S3 Public Write Rule	Yes	Enable check for S3 buckets with public write enabled Config Rule?
Enable S3 SSE Policy Rule	No	Enable S3 bucket policy check for Server Side Encryption Config Rule?
Enable Root MFA Rule	Yes	Enable root user MFA Config Rule?
Enable IAM Password Policy Rule	Yes	Enable IAM password policy Config Rule?
Enable Restricted Common Ports Rule	Yes	Enable Amazon EC2 restricted common ports Config Rule?
Enable Restricted SSH Rule	Yes	Enable Amazon EC2 restricted SSH Config Rule?

11. Choose **Next**.
12. On the **Options** page, choose **Next**.
13. 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.
14. Choose **Create** to deploy the stack.
15. 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.