Deleting the AWS Landing Zone - DRAFT

The following process will delete a successfully deloyed AWS Landing Zone from your Master Account. If you are trying to delete the solution from and incomplete deployment, you may need to manually delete components. If you need to do so, please attempt to maintain the order outlined below.

1. If you connected the directory in SSO, you MUST disconnect the directory before continuing.
    a. Change to the us-east-1 region
    b. Navigate to the SSO Service -> Connected Directory
    c. Disconnect the Directory from SSO
        i. Remove all assignments and disconnect
    d. Switch back to your primary region

2. Delete Provisioned Products from Service Catalog
    a. Switch back to your primary region
    b. Navigate to the Service Catalog - > Provisioned Products List
    c. Switch the View from User to Account
    d. Terminate the following Provisioned Products by clicking the 3 dots next to the product
        i. lz_core_*
    e. Navigate to Cloudformation and you should see lots of stacks deleting

3. Remove Products from Portfolios in Service Catalog
    a. Navigate to Service Catalog
    b. For each portfolio in “Portfolios List” i.e. “AWS Landing Zone Core” and “AWS Landing Zone – Baseline”
        i. Delete all Constraints
        ii. Delete all Users and Groups
        iii. Remove the product from the portfolio
        iv. Navigate to the Portfolios List
        v. Delete the portfolio

4. Delete Products from Service Catalog
    a. Navigate to Service Catalog
    b. For each product in “Products List” i.e. "AWS Centralized Logging Solution" and "AWS-Landing-Zone-Account-Vending-Machine"
        i. Delete Product

5. Delete all CloudFormation Baseline Stacks
    a. Navigate to Cloudformation
    b. Select all stacks with “SO0045” in the description.
    c. Delete Stacks. These can be done in parallel.

6. Delete the Security Baseline for each account via StackSets in the Master Account
    a. Navigate to Cloudformation StackSets
        I. Delete the following StackSets in parallel

II. AWS-Landing-Zone-EnableCloudTrail
III. AWS-Landing-Zone-EnableConfig
IV. AWS-Landing-Zone-EnableConfigRules
V. AWS-Landing-Zone-EnableNotification
VI. AWS-Landing-Zone-IamPasswordPolicy

7. For the remaining StackSets which will still have stack instances, you will need to Manage Stacksets, enter the account numbers and regions, and delete all stack instances. Once the stack instances have been deleted, delete the StackSets as follows.
    a. Delete Instances in StackSet “AWS-Landing-Zone-SharedTopic” then delete the StackSet.
    b. Delete Instances in StackSet “AWS-Landing-Zone-SharedBucket” then delete the StackSet.
    c. Delete Instances in StackSet “AWS-Landing-Zone-SecurityRoles” then delete the StackSet.
    d. Delete Stack Instances in StackSet “AWS-Landing-Zone-PrimaryADConnector” then delete the StackSet. Wait for this to complete.
    e. Delete Stack Instances in StackSet “AWS-Landing-Zone-PrimaryAccountVPC” then delete the StackSet.
    f. Delete Stack Instances in StackSet “AWS-Landing-Zone-SharedServicesRDGW” then delete the StackSet.
    g. Delete Stack Instances in StackSet “AWS-Landing-Zone-SharedServicesActiveDirectory” then delete the StackSet.
    h. After the RDGW and AD StackSets have been deleted, delete Stack Instances in the StackSet “AWS-Landing-Zone-SharedServicesAccountVPC” then delete the StackSet.

8. Delete the following S3 buckets in the Master Account
    a. Navigate to the S3 Service
    b. Delete the following buckets
        i. aws-landing-zone-configuration-<accountid>-<region>
        ii. initiationtemplate-landingzonepipelineartifacts*

9. Delete the Logging Bucket in the Logging Account (Note: In case you have locked the StackSet Execution Role, follow steps on Appendix A)
    a. Switch role to the Logging account
    b. Navigate to S3
    c. Delete the following buckets
        i. stackset-aws-landing-zone-sharedbucket--s3bucket-*
    d. Switch back to the primary account

10. Delete the Landing Zone initiation template
    a. Navigate to CloudFormation
    b. Select the Initiation stack
    c. Delete the stack
    d. If there are issues with deletion of resources, delete them manually and retry the stack deletion until successful

11. Clean up Organizations
    a. Move the following accounts out of the Core OU back to Root
        i. Primary
        ii. Shared Services
        iii. Logging
        iv. Security
    b. Delete the Core and Application OUs
    c. Delete the Service Control Policy
        i. protect-cloudtrail-config

12. Delete all the Landing Zone SSM Parameters
    a. Navigate to Systems Manager -> Parameter Store
    b. Delete all parameters

13. Ensure the Landing Zone KMS Keys have been deleted
    a. Navigate to IAM -> Encryption Keys
    b. Delete the key if you want to remove LZ permanently
    c. If you plan on reinstalling LZ, DO NOT REMOVE THE KEY

Appendix A

How do I unlock my member account to be able to switch roles from the master/primary account?

1. Reset the root password for the Security account

2. Login to the Security account using root credentials.

3. Navigate to the IAM console and click on the role "AWSCloudFormationStackSetExecutionRole".

4. Click on the "Trust Relationships" tab.

5. Click on the "Edit Trust Relationships" button.

6. Edit the principal to "arn:aws:iam::MASTER_ACCT:root" (this will unlock the account, and you will be able to switch from the master/primary account)

7. Use Security account to switch role to "Shared Services" and Logging" account using role name "AWSLandingZoneAdminExecutionRole" and perform Steps 3-6 for each account.

8. Logout of Security Account and log back into Master account to continue deletion process.