aws marketplace

Implementation Guide:

Multi account entitlements governance in AWS with Ermetic and AWS Control Tower

Table of Contents

Foreword

Ermetic is an "identity-first" cloud security platform that helps organizations secure public cloud infrastructure across the full stack of identities, network, data, and compute resources. Ermetic helps reduce the attack surface by continuously analyzing permissions, configurations, and behavior across the full stack of identities (human and service), entitlements, data, network, and compute resources.

This Implementation Guide describes how AWS Marketplace customers can automatically extend Ermetic's capabilities to new accounts added via AWS Control Tower.

Solution overview and features

Ermetic enables management of AWS cloud identities and resources in one unified platform where you can investigate entitlements, configurations, and relationships between identities.

This template provisions infrastructure in the Control Tower management account that allows creation of an Ermetic IAM integration role in Control Tower managed accounts whenever a new Control Tower managed account is added.

- Creates a Ermetic Stackset in the Control Tower management account
- Provisions a CloudWatch Events Rule that is triggered based on a Control Tower Lifecycle Event
- Provisions a Lifecycle Lambda as a target for the CloudWatch Events Rule
- The Lifecycle Lambda deploys an Ermetic stack that onboards the newly added Control Tower managed account to Ermetic

Architecture diagram

The solution is deployed using AWS CloudFormation templates and integrates with AWS Control Tower Lifecycle events. When a new account is created, or an existing one is enrolled using the AWS Control Tower Account Factory, the Lifecycle event triggers a Lambda function. The Lambda function creates a new CloudFormation stack instance in the vended account, creating the required IAM role in the newly vended account.

The stack instance configures Ermetic with an IAM role to collect account data from IAM, resource id/tags, and CloudTrail logs from the new account.

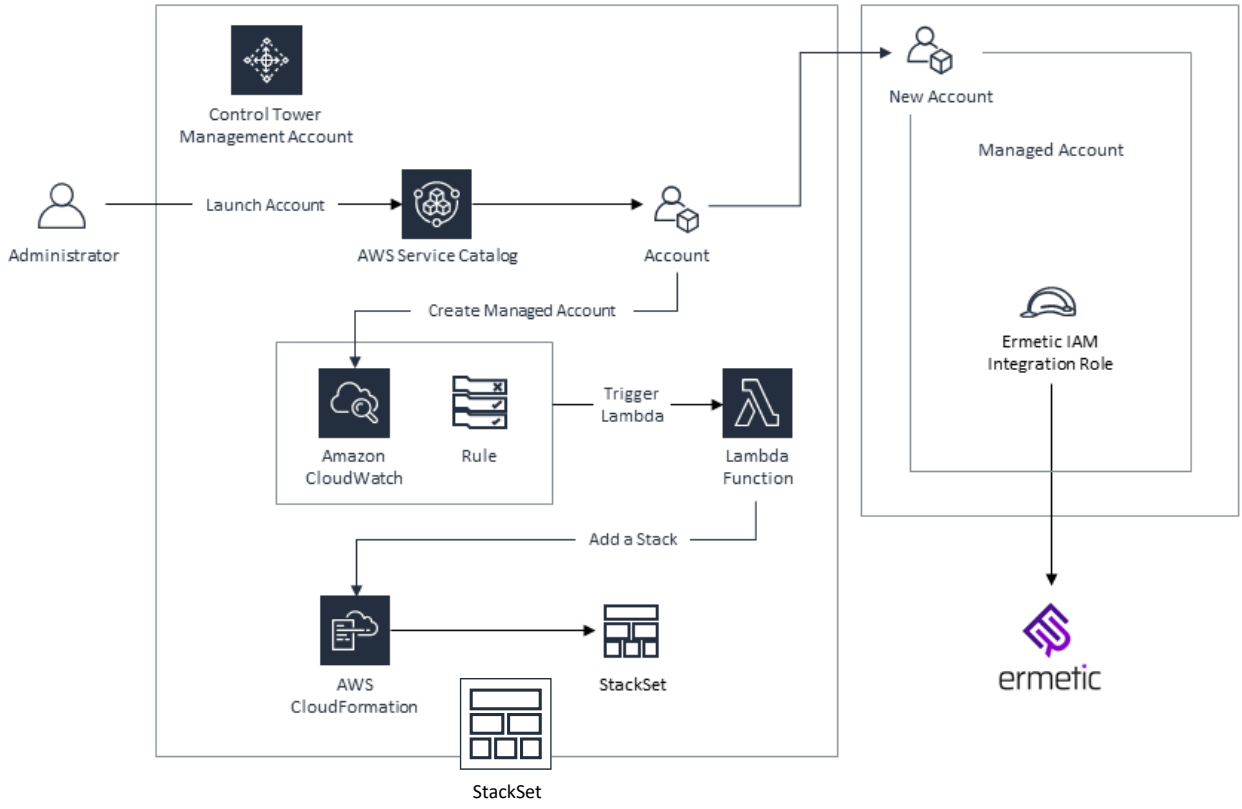


Figure 1 Ermetic Control Tower Architecture Diagram

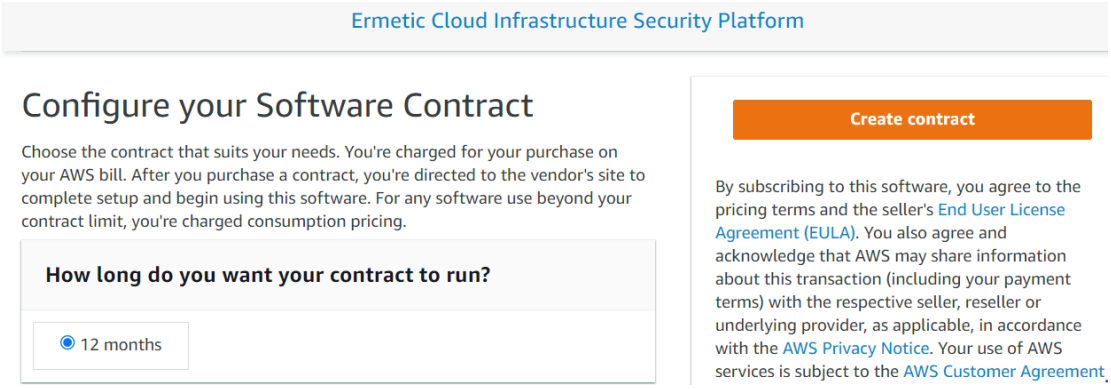
Deployment and Configuration Steps

The solution can be found in the Ermetic Control Tower GitHub repository. It uses two AWS CloudFormation templates that you will deploy in your AWS Control Tower management account. These templates include all the components required to integrate Ermetic with new AWS accounts that you create using the AWS Control Tower Account Factory.

Step 1: Ermetic - Initial Setup

1. Subscribe to Ermetic via the AWS Marketplace
    a. From AWS Marketplace
    b. Choose **Continue to Subscribe**

    c. Click **Create Contract**



Step 2: AWS Setup – AWS Control Tower management account

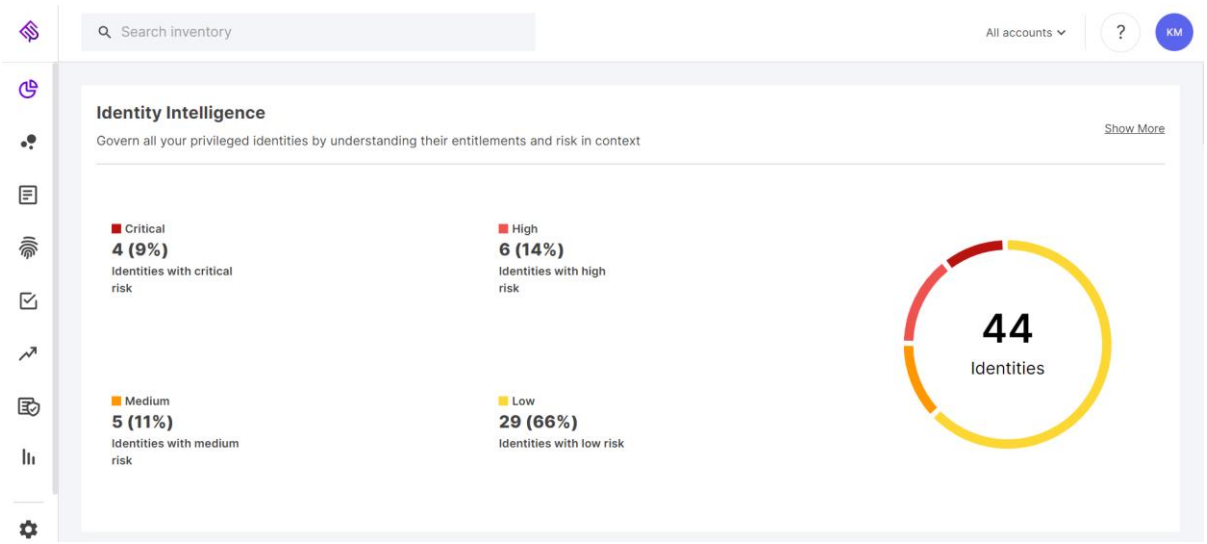
1. Launch the aws-ermetic-controltower.yaml template in the AWS Control Tower Managed account
    a. Ensure that an AWS CloudFormation StackSet is successfully created
    b. Ensure that an Amazon CloudWatch Events rule is successfully created with an AWS Lambda target to handle Control Tower lifecycle events

Step 3: Test - Create a Lifecycle Event - Add a managed account

1. From the AWS Control Tower Master Account:
    a. Use Account Factory or quick provision or Service Catalog to create a new managed account in the AWS Control Tower Organization OR
    b. Use Service Catalog (AccountFactory Product) to update an existing managed account - for e.g. change the OU of an existing managed account
    c. This can take up to 30 mins for the account to be successfully created and the AWS Control Tower Lifecycle Event to trigger
    d. Login to the AWS Control Tower managed account –
        i. Validate that an AWS CloudFormation stack instance has been provisioned that launches the Cribl LogStream single instance template in the managed account.

Step 4: Complete the onboarding of the new managed account in Ermetic

1. Sign in your Ermetic account and select **Settings** from the left panel, select **Accounts** and then select **Add a new AWS account.** Skip steps 1, 2 and 3 since we have already provisioned the IAM role in the new account. For step 4, provide the Account ID of the new managed account (Managed Account ID) and the ARN of the newly provisioned IAM role in the managed account (arn:aws:iam::<Managed Account ID>:role/IAM_R_ERMETIC_SECURITY_XA)
2. Select “Continue without CloudTrail’ since we will use the centralized CloudTrail from Control Tower and click Finish



Solution Estimated Pricing

Contact Ermetic Team to learn more.

FAQs

You can find a list of FAQs for the Ermetic product and integrations in our documentation here.

Additional resources

- Ermetic AWS Solutions Page

Partner contact information

For general inquiries, contact support@ermetic.com.