

Implementation Guide:

Sonrai Dig - Identity and Data Governance for AWS Control Tower



Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram	5
Pre-requisites	7
Deployment and Configuration Steps	8
Subscribe to Sonrai Security	8
Getting started	9
What to expect	10
Use Case	11
Best Practices	14
Solution Estimated Pricing	14
Additional resources	14
Read our case studies:	14
Partner contact information	14

Foreword

Sonrai Dig is an award-winning <u>enterprise identity and data governance platform</u> that is built on a sophisticated graph that helps you to continuously identify and monitor every possible relationship between identities and data that exists inside your AWS environment. Sonrai Dig's Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and security teams to ensure end-to-end security on the AWS cloud. By implementing this solution, your organization can eliminate identity risks getting to and maintaining the Least Privilege access.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Sonrai Dig in an AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

As your enterprise shifts to the cloud to increase efficiency, concerns for risk in access and privilege management, configuration drift, and sensitive data loss need to be addressed. Sonrai Dig's Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and development teams to ensure end-to-end security.

With the Sonrai Security platform, your enterprise can:

- ✓ Reduce Risk with Sonrai Dig on AWS to eliminate risk and secure Amazon Elastic Compute Cloud (EC2) instances and other AWS services across multiple accounts with patented graph analytics, superior integrations, and intelligent collection to find identity, data, and network risks.
- ✓ Increase Security with continuous access monitoring to prevent security breaches. The Sonrai Dig data and identity-centric security approach finds, classifies, minimizes access, and continuously monitors all Crown Jewel data in structured and unstructured stores.
- ✓ Enforce compliance with over 1000 control policies and 30 frameworks spanning data, identity, cloud-platform, and container compliance regulations, including General Data Protection Regulation (GDPR), Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST), and more. Sonrai Dig on AWS is the most comprehensive cloud and security continuous compliance platform.
- ✓ Maximize efficiency and automate security policies across multiple accounts and environments, as you migrate or create new workloads. Utilize machine learning and graph analytics that automate identifying, classifying, and prioritizing by routing risks to the teams and individuals responsible.

Sonrai Dig's integration with AWS Control Tower enables customers to automatically protect existing and newly enrolled AWS Accounts through a series of automation in response to an AWS Control Tower Lifecycle events:

- Perform pre-requisite steps to setup Sonrai Dig in the AWS account vended by AWS Control Tower Account Factory
- Register an AWS account in Sonrai Dig portal to initiate ingestion set-up.
- Set up ingestion of AWS CloudTrail logs into Sonrai Dig platform.
- Sonrai Dig finds accounts that are part of your organization to ensure compliance and security controls are enforced protection scope by Sonrai Dig.

Architecture diagram

Enterprise organizations require security throughout their software development lifecycle (SDLC) that will automatically monitor and protect their workloads when migrating or developing in the cloud. To reduce risk, organizations need to govern all identity and data relationships between people and non-people identities (admins, roles, compute instances, serverless functions, and containers) across multi-cloud accounts and 3rd-party data stores and relentlessly monitor critical data sitting inside object stores and database services. Suspicious access activity or undesirable changes in access rights must be flagged.

Sonrai Dig provides an identity and data governance platform built for cloud and container environments, providing end-to-end visibility across your entire cloud. Our Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and security teams to ensure end-to-end security.

Sonrai Dig's integration with AWS Control Tower configures each AWS Control Tower managed account during launch, then leverages the CloudWatch Event triggered when a managed account is created to trigger customization of the member account. The AWSControlTowerExecutionRole in each account is then used to create access for Workload Security.

This integration of Sonrai Dig utilizes the following AWS Services to enable automatic protection of existing or newly enrolled AWS Accounts: Amazon EventBridge, AWS CloudFormation, AWS Lambda, and AWS IAM.

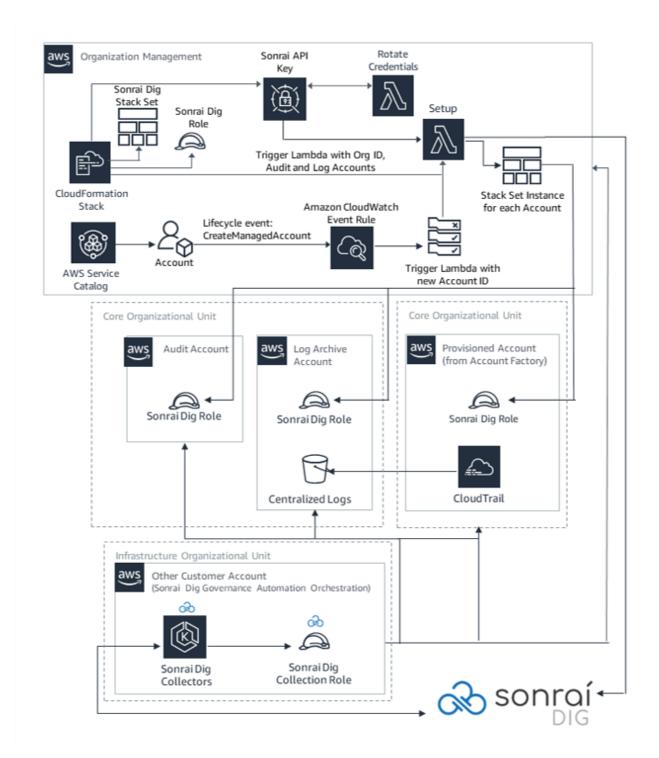
AWS Accounts presented in the architecture diagram are:

- Management Account Management account on which AWS Control Tower was enabled.
- Log Archive Account Account for a centralized repository of logs including CloudTrail logs.
- Audit Account Restricted account with read/write access to all accounts. Centralized topic for security and CloudTrail notification are located here.
- Security Account An account where Sonrai Dig Governance Automation Orchestration is deployed, and the Sonrai Dig Collectors are configured.

Provisioned Account(s) – Additional accounts in the organization.

Deployed as part of this integration are the following:

IAM Role that allows Sonrai Dig deployed collectors access to accounts managed by Control Tower



Pre-requisites

Before deployment it is required that you have a current Sonrai Dig account. If you do not have a Sonrai Dig

Collectors

subscription, please check the listing on AWS Marketplace.

The solution requires a dedicated AWS account to be designated as a Security account. Additionally, you must have deployed a Sonrai Dig into your Security account and have it configured to be scanning your organization. To configure Sonrai Dig Collectors please navigate to "Collectors" in the Sonrai Dig platform.

Detailed instructions are available here

(https://s3.amazonaws.com/sonrai-

kb/crc/guides/sonrai aws intel collector-configuration guide.pdf)

When deploying collectors take note of the following as they will be needed for the AWS Control Tower integration:

- AWS Account number the collectors are deployed into (your security account)
- The name you gave the deployment in the Sonrai Dig platform
- The external ID assigned to that deployment (Obtained by pressing the Create Role buttons in collector configuration)

This guide assumes you already have AWS Control Tower deployed. To get started with AWS Control Tower, check out the <u>Getting Started</u> documentation. Before you implement this solution, we recommend that you become familiar with AWS CloudFormation, AWS Lambda and Amazon EventBridge services.

If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started/.

For additional information on AWS Marketplace, see https://aws.amazon.com/marketplace/help/about-us?ref = footer nav about aws marketplace.

To get started with AWS Control Tower, check out the

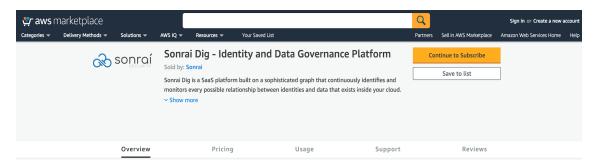
https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html

Deployment and Configuration Steps

Subscribe to Sonrai Security

Step 1.1: Subscribe to Sonrai Security on AWS Marketplace.

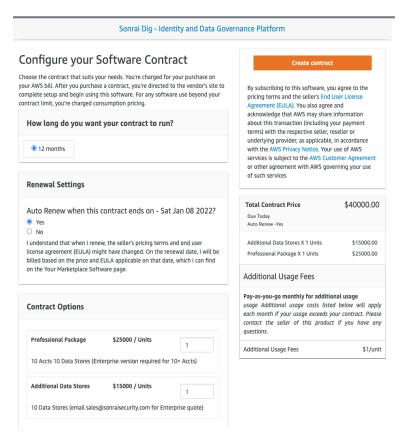
Locate Sonrai Dig in the AWS Marketplace (https://aws.amazon.com/marketplace/pp/B07ZQNZZVT).



Click on the Continue to Subscribe button.

Step 1.2: Guidance on Contract Duration and Renewal

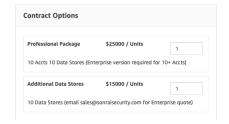
In the new screen, you can configure your contract. Select the **Contract Duration** and set the **Renewal Settings** of your choice.



Step 1.3: Select Contract Options

Select the Contract Options to be activated with your contract.





Step 1.4: Create the Contract and Pay

Once you have configured your contract, you can click on the Create contract button.

You will be prompted to confirm the contract. If you agree to the pricing, select the Pay Now button.

Step 1.5: Set up Account

Sonrai will create a customer tenant and the Sonrai Customer Success team will contact the customer for set-up, deployment, and onboarding.

Step 2.1: Log into the Sonrai Security

Go to https://crc.sonraisecurity.com/Login to login to Sonrai Dig.

Getting started

Step 3.1: Generate an API token for the Sonrai Dig platform (ensure the user generating the keys will have enough permissions to configure collectors to add new accounts). API tokens are generated via Sonrai Dig GraphQL api (https://crc.sonraisecurity.com/App/GraphExplorer), paste in the following and execute:

```
mutation createToken {
  GenerateSonraiUserToken (input:{
    expiresIn: 2592000
    name: "Control Tower Integration"
  }) {
    expireAt
    token
  }
}
```

Copy the value of "token" to be used in Step 3.3

Step 3.2: Create a new CloudFormation stack in your Organization Management account using the following URL:

https://console.aws.amazon.com/cloudformation/home?#/stacks/create/template?templateURL=https://sonrai-global-artifacts-

public.s3.amazonaws.com/control_tower_integration/cf_templates/setup.yaml&stackName=SonraiDigCTDeploy

Source Code for templates and lambdas can be found here: https://github.com/sonraisecurity/control-tower-integration

Step 3.3: Enter the following from the prerequisite step and Step 3.1:



- Sonrai Dig Configuration:
 - Sonrai Dig Collector Deployment Name: from prerequisites
 - o Sonrai Dig Collector Role External Id (UUID): from prerequisites
 - Sonrai Dig Collector Account Number: from prerequisites
 - Sonrai Dig API token: from step 3.1
- Organization Configuration
 - o Organization Id: AWS Management Account, AWS Organizations, Settings
 - Audit Account Number: AWS Organizations, Accounts, Audit
 - Log Archive Account Number: AWS Organizations, Accounts, Log archive
- Deployment Configuration
 - Source Bucket: sonrai-global-artifacts-public (default)
 - Stack Set Name: SonraiDigAccess (default)
- Other parameters
 - o Role Name: sonrai-collector-role (default)

Step 3.4: Once the stack has been created the solution will be deployed

What to expect

Step 4.1: In the Core accounts as well as any other accounts in the organization you should now see an additional IAM Role with a trust relationship to your Security account with the external Id provided. Additionally, the Rotate Credentials Lambda function will keep the Sonrai Dig credentials up to date using the secret rotation functionality of AWS Secrets Manager

Step 4.2: How to use:

As the Sonrai Dig platform will be monitoring your organization for changes, any accounts that exist or accounts added to the organization in future are automatically added to the list of accounts scanned. The AWS Control Tower lifecycle events are used to detect the new AWS Account creation and create the IAM roles that grant the scanning access.

Use Case

Detect and show remediation of IAM policies that allow privilege escalation, including over privileged users/roles, help move to least privilege

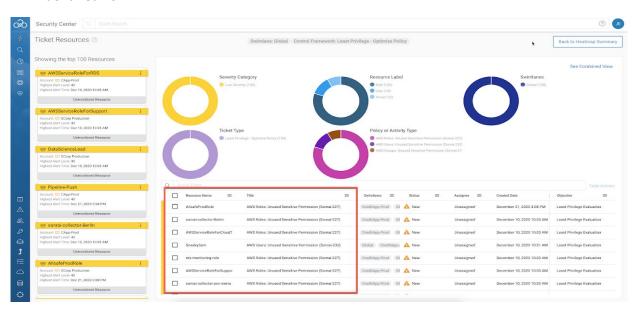
The Sonrai platform helps customers achieve a "Least Privilege" state across all their public cloud environments. Sonrai built the automated permission modeling graph using machine learning to achieve the least privileged state. This model examines all users, roles, trusts, policies, permissions, non-person identities, groups, etc., and maps out all possible "Effective Permissions".

This exposes worst-case scenarios, and ultimately the blast radius should an Identity become compromised. Sonrai then monitors used vs. unused privileges to then recommend an optimized "Least Privilege" policy.

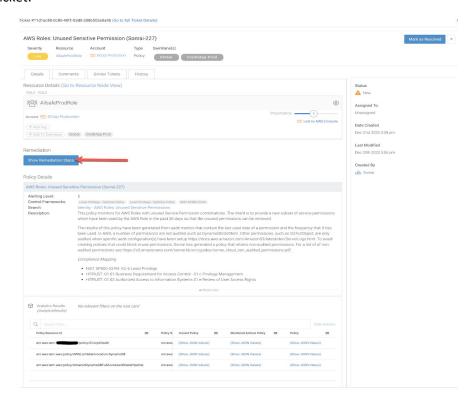
1. In this use case we have enabled 4 "Least Privilege" IAM control frameworks here that focus on Unnecessary permissions for AWS Administrators, Policies, Roles and Service Admins:



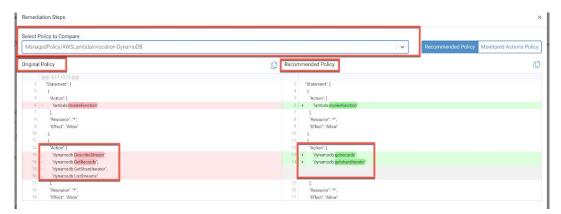
2. Click on the Global Swimlane for the "Optimize Policy" control framework and you will see all identified risk:



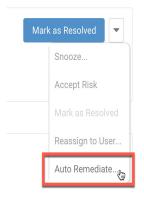
- 3. You can see in the above screenshot all the Resources that Sonrai has identified for excessive permissions across AWS Roles, Users and Groups.
- 4. Clicking into the first Resource identified you can see very specific details regarding the risk in the Alert ticket:

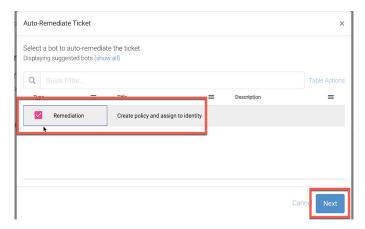


- 5. Clicking the "Show Remediation Steps" button reveals the original policy on the left and the optimized least privilege policy on the right. You can choose the various policy recommendations for this Role by using the drop-down bar at the top.
- 6. You can see how Sonrai examines all used permissions and recommends a better "Least Privilege" policy on the right, only assigning the Role the exact permissions it needs to function.



7. To implement the optimal policy, just choose the auto-remediation option from the available drop-down menu of ticket workflow options and select the appropriate remediation bot:





This tutorial is an overview of how Sonrai's patented Graphing technology can discover and expose complex permission chaining. These chains result in toxic permissions, privilege escalation, cross-account access, and other unintentional escalated privileges. Sonrai can monitor and learn which permissions are truly necessary and then recommend optimal least privilege policies for both person and non-person identities.

Best Practices

- Sonrai Security Knowledge Base and Help Center
- Sonrai Security User Guides

Solution Estimated Pricing

There are no Sonrai Security pricing implications as the Sonrai Dig solution provides asset visibility to Sonrai Security which is free. Once the discovered assets are scanned then normal Sonrai Dig pricing is in effect.

Public pricing for Sonrai Security is available on <u>AWS Marketplace</u>: https://aws.amazon.com/marketplace/pp/B07ZQNZZVT

Additional resources

Get more information on <u>Sonrai Dig platform</u>

Try our <u>Cloud Security Assessment</u>

Learn more about <u>Sonrai Dig on AWS</u>

Visit the Sonrai Security listing on the <u>AWS Marketplace</u>

Read our case studies:

World Fuel Services Case Study
Snoop Case Study
Risk Management Solutions Case Study

Partner contact information

For questions regarding Sonrai Dig or Sonrai Security offerings on AWS Marketplace, please email us at awsteam@sonraisecurity.com or visit https://sonraisecurity.com/contact-us/

For customer support, contact us via email.