

Table of Contents

Cloud Onboarding

Onboard AWS	2
-----------------------------------	---

Onboard AWS

Onboard your entire AWS organization or individual accounts in Tenable Cloud Security to get full visibility and risk assessment for all cloud identities and resources associated with the organization/account, including information about permissions, account usage, and security configurations. Tenable collects inventory and configuration data from AWS API, and activity data from AWS CloudTrail logs.

- [Onboard Your AWS Organization](#)
- [Onboard an Account](#)

After you complete onboarding, Tenable Cloud Security displays a [status for each account](#), indicating, for example, whether Tenable can connect to the account, and helping you troubleshoot potential onboarding issues.

See [Account Architecture](#) for a visual overview of the IAM trust relationship that is established during onboarding, including required permissions. See [AWS FAQs](#) for a list of frequently asked questions related to AWS onboarding.

It's important to fully understand the implications of CloudTrail pricing before onboarding accounts. Refer to [AWS CloudTrail Pricing](#) for official, updated pricing information.

- AWS charges for both management and data events.
- AWS grants one free trail that delivers a single copy of management events in each region, for a given account.
- Additional rates apply for any data event and for additional copies of management events beyond the first copy in each region.
- Tenable Cloud Security contributes to the number of total management events.
- **As a best practice to avoid unnecessary fees, Tenable Cloud Security recommends using either a single organization trail or one trail per account to capture events across all accounts. This ensures that you are not charged for management events for additional trail copies.**

Considerations for Onboarding an Organization Versus Individual Accounts

When deciding whether to onboard your entire AWS organization as opposed to individual accounts, it's important to consider how this decision impacts features in Tenable Cloud Security. Tenable recommends onboarding your entire organization to ensure that the management account is connected to Tenable, and to avoid losing visibility related to the following features/capabilities:

- **AWS Identity Center (formerly AWS SSO)** - *Affects visibility into users, groups, permission sets, and their effective use, as well as least-privilege recommendations.*
- **Service control policy (SCPs)** - *Limited entitlement visibility.*
- **Cross account visibility** - *Tenable won't be able to differentiate between accounts that are part of your organization (but not onboarded) and those that are not.*
- **Least privilege** - *Tenable won't be able to provide the most accurate recommendations.*

Onboard Your AWS Organization

Onboard your entire AWS organization to expedite and automate the onboarding process in cloud environments with many accounts. Doing so allows you to:

- Simultaneously onboard all accounts to Tenable at once.
- Automatically onboard new accounts added in AWS at a later stage.
- Ensure visibility related to the full range of platform features (see [Considerations for Onboarding an Organization Versus Individual Accounts](#)).

Prerequisites:

- [Onboard your management account](#) to Tenable Cloud Security.

To onboard an AWS organization:

Be aware that during the wizard you will need to navigate back and forth between the Tenable Cloud Security Console and the AWS Management Console.

1. In the Tenable Cloud Security Console, navigate to **Settings > Integrations** and click on **AWS Organization**.
2. Click **Lets Start**. The Add AWS Organization wizard opens.
3. **Select a management account**. You'll need to [add the account](#) to Tenable for it to appear in the dropdown.
4. Enter organization details:
 - a. Verify that the **Organization Name** and **Role Name** are correct.

- The **Organization Name** is the ID of the organization, and can be found in the AWS Organizations console.
- If you previously onboarded individual accounts to Tenable Cloud Security, make sure that the name of the IAM role you choose here is different than any role names used for those accounts. After deploying the StackSet later on in this wizard, you can safely remove any other roles that were used.

- b. Select the **CloudTrail Name** to be used in all member accounts, assuming you are using a default name for member accounts. If you aren't using a default name for CloudTrails in all member accounts, you can still configure CloudTrail for individual accounts, after organization onboarding. You can enter a wildcard character (*****) in this field (e.g. `Organization-Trail-*` would select `Organization-Trail-1234`).

After organization onboarding is complete, you still need to grant Tenable access to the S3 bucket containing the trail. To do so, in Tenable Cloud Security, edit the relevant account where the bucket is located and grant Tenable CloudTrail permissions via the IAM role. If the bucket is located in your management account, you may have already done this during initial account onboarding.

- c. Select all relevant **Active Regions** where you have resources deployed.

Verify that you select only the specific regions used by your organization. Unselected regions will be ignored. Enable all regions not disabled or blocked by SCPs for scanning. If your deployment expands to additional regions at a later stage, you will need to edit the account in Tenable Cloud Security and add those regions.

- d. Choose whether to **automatically update folder structure**.

Copy your AWS organizational unit folder structure into the platform, keeping your account hierarchy intact and continuously synchronized. Learn more about [account hierarchy](#).

- e. Choose whether to **create a dedicated folder for the organization**.

Select this option if you are planning to onboard multiple AWS organizations. This will create a dedicated folder for the AWS Organization in the platform. If you don't plan to onboard more than one organization, unselect the checkbox.

5. Click **Next**.

6. Choose **Permissions** (Step 3 in wizard). Choose which features to enable, keeping in mind that each feature requires different permissions. You can modify your selection after the initial onboarding. See [Required Permissions](#) to learn more about why Tenable needs these permissions granted. When finished, click **Next**.

- **Monitoring** (read-only). Gain full visibility for all cloud assets, including information about permissions, account usage, and security configurations. Additional permissions may be required to read the CloudTrail for the onboarded account.
- **Remediation** (read-write). Allow Tenable to make changes in your environment. This lets you automatically remediate findings with one click, for example (One-click remediation is still available via OTP without these permissions).

- **S3 Bucket Scanning (Data Protection).** Scan objects in public S3 buckets for sensitive data.

Public bucket scanning is included with the Standard/Enterprise license. No additional configuration is required.

- **Private S3 Bucket Scanning (Data Protection).** Scan objects in private S3 buckets for sensitive data.

Relevant if you're working with Tenable Cloud Security Data Protection (requires Enterprise license). See [Data Protection](#) for more information. See [the appendix](#) to view the policy in JSON format.

- **EC2 Instance Scanning (Workload Protection).** Scan EC2 Instances for vulnerabilities and misconfigurations.

Relevant if you're working with Tenable Cloud Security Workload Protection (requires Standard/Enterprise license). See the relevant [Workload Protection documentation](#) for more information. See [the appendix](#) to view the policy in JSON format.

- **ECR Scanning (Workload Protection).** Scan container registries for vulnerabilities and misconfigurations.

Relevant if you're working with Tenable Cloud Security Workload Protection (requires Standard/Enterprise license). See the relevant [Workload Protection documentation](#) for more information. See [the appendix](#) to view the policy in JSON format.

7. Create a new **IAM role** (Step 4 in wizard) using **CloudFormation** (via either the AWS Console, or the AWS CLI):

- **CloudFormation (AWS Console):**

- a. Log in to the AWS management account for your organization.

- b. Navigate to **CloudFormation > StackSets**.
- c. Click **Create StackSet**.
- d. In Step 1 (Choose a template), keep the default values in the *Permissions* and *Prerequisite - Prepare Template* sections, and, in the *Specify Template* section, enter the following **Amazon S3 URL**:
`https://tenable-utilities.s3.us-east-2.amazonaws.com/Onboarding/AWS/CloudFormation/Template.json`
- e. Click **Next**.
- f. In Step 2 (Specify StackSet details), enter a **StackSet name**, and, optionally, a description.
- g. Enter the parameter values listed in the Add AWS Organization wizard in the Tenable Cloud Security Console.
- h. Click **Next**.
 - i. In Step 3 (Configure StackSet options), keep the default values as they are, and click **Next**.
 - j. In Step 4 (Set deployment options), choose either **Deploy to organization** or **Deploy to organizational units (OUs)**, as relevant. Keep the other default values as they are.
 - k. In the *Specify Regions* section, choose a single region (IAM roles aren't regional).
 - l. Click **Next**.
- m. In Step 5 (Review), review the StackSet configurations. Select **I acknowledge that AWS CloudFormation might create IAM resources with custom names** and then click **Submit**.
- n. Wait until the Stack creation is complete. You can click on the **Refresh** button to track progress.
- o. [Tenable Cloud Security Console] Click **Finish**.

○ **CloudFormation (AWS CLI):**

- a. Log in to the AWS management account for your organization.
- b. Open a new shell session with the latest version of the **AWS CLI**`{target='_blank'}`. Administrator privileges are required to create the CloudFormation stack


- c. Copy the command that appears in the Tenable Cloud Security Console, and run it in your shell.
- d. In the AWS Management Console, navigate to **CloudFormation > StackSets** and open the newly created StackSet.
- e. Wait until the Stack creation is complete. You can click on the **Refresh** button to track progress.
- f. [Tenable Cloud Security Console] Click **Finish**.

Onboard an Account

Use this procedure to onboard an individual account. If you are [onboarding your entire AWS organization](#), you will need to first follow this procedure to onboard the management account individually before continuing to onboard the organization.

To onboard an AWS account to Tenable:

Be aware that during the wizard you will need to navigate back and forth between the Tenable Cloud Security Console and the AWS Management Console.

1. In the Tenable Cloud Security Console, navigate to **Accounts > AWS** and click  and then **Add account**. The Add Account wizard opens.

If you haven't configured any accounts yet, click **Lets Start**.

2. [Tenable Cloud Security Console] Enter **Account Details** (Step 1 in wizard):
 - a. Enter a **Name** for your account. This name will be used in the Console.

You can choose whether to use the same naming convention in both the AWS Management Console and the Tenable Cloud Security Console. If you do use different names, make sure you can map the account names across the different consoles.

- b. Verify that the appropriate **AWS Partition** is selected (AWS Global or AWS China). The partition that your AWS account belongs to. A partition is a group of AWS Regions. For more information, refer to [AWS Documentation](#).
- c. Select all relevant **Active Regions** where you have resources deployed, and then click **Next**.

Verify that you select only the specific regions used by your organization. Unselected regions will be ignored. Enable all regions not disabled or blocked by SCPs for scanning. If your deployment expands to additional regions at a later stage, you will need to edit the account in Tenable Cloud Security and add those regions.

- 3. [Tenable Cloud Security Console] Choose **Permissions** (Step 2 in wizard). Choose which features to enable, keeping in mind that each feature requires different permissions. You can modify your selection after the initial onboarding. See [Required Permissions](#) to learn more about why Tenable needs these permissions granted. When finished, click **Next**.
 - **Monitoring** (read-only). Gain full visibility for all cloud assets, including information about permissions, account usage, and security configurations. Additional permissions may be required to read the CloudTrail for the onboarded account. For more information about required permissions, see the documentation.
 - **Remediation** (read-write). Allow Tenable to make changes in your environment. This lets you automatically remediate findings with one click, for example (One-click remediation is still available via OTP without these permissions). For more information about required permissions, see the documentation.
 - **Just-in-time Access** (AWS Identity Center). Grant users access to cloud accounts for a predetermined period of time and on an as-needed basis. If the account you are onboarding is the management account, or has permissions to manage AWS Identity Center, additional permissions are required. For more information about required permissions, see the documentation.
 - **S3 Bucket Scanning (Data Protection)**. Scan objects in public S3 buckets for sensitive data.

Public bucket scanning is included with the Standard/Enterprise license. No additional configuration is required.

- **Private S3 Bucket Scanning (Data Protection).** Scan objects in private S3 buckets for sensitive data.

Relevant if you're working with Tenable Cloud Security Data Protection (requires Enterprise license). See [Data Protection](#) for more information. See [the appendix](#) to view the policy in JSON format.

- **EC2 Instance Scanning (Workload Protection).** Scan EC2 instances for vulnerabilities and misconfigurations.

Relevant if you're working with Tenable Cloud Security Workload Protection (requires Standard/Enterprise license). See the relevant [Workload Protection documentation](#) for more information. See [the appendix](#) to view the policy in JSON format.

- **ECR Scanning (Workload Protection).** Scan container registries for vulnerabilities and misconfigurations.

Relevant if you're working with Tenable Cloud Security Workload Protection (requires Standard/Enterprise license). See the relevant [Workload Protection documentation](#) for more information. See [the appendix](#) to view the policy in JSON format.

- **CloudTrail (S3).** To analyze cloud activity logs, permissions are required to read from the S3 bucket storing CloudTrail data. If the bucket belongs to the account you are currently onboarding, select this option. For more information, see [CloudTrail Logs](#).
 1. Enter the **Bucket name** where the trail data is stored.
 2. Indicate whether the trail bucket is **encrypted with AWS KMS**, and if so, enter the **KMS key ARN**.

If the bucket belongs to a different account, you will need to do one of the following after completing this wizard:

1. *[When only onboarding individual accounts]*
Onboard the other account separately and grant **Tenable CloudTrail** permissions via the IAM role.
2. *[When onboarding your entire organization]*
Complete organization onboarding, and then edit the relevant account and grant **Tenable CloudTrail** permissions via the IAM role.

- **Terraform State (S3).** To analyze Terraform resources, permissions are required to read from the S3 bucket storing the state data.

Relevant in you're working with IaC, and you want to trace issues back to code. This permission can only be enabled by editing the account, after successful onboarding. See [Trace Issues Back to Code](#) for more information.

4. Create a new **IAM role** (Step 3 in wizard), using either **CloudFormation** (via the AWS Console, or the AWS CLI) or **manually** in the AWS Console:

- **CloudFormation (AWS Console):**

1. Log in to the AWS account that you want to onboard.
2. [Click here](#) to create a Stack, and then perform the following steps in the AWS Create stack wizard:

You can use the link provided here, or the link in the wizard. However, if you use the link provide here, verify that the true/false values for each of the Tenable Policies reflect the permissions that you chose in step 2 of the wizard.

3. (Optional) Choose a different name for the IAM role by modifying the **RoleName** parameter.
 4. Select *I acknowledge that AWS CloudFormation might create IAM resources with custom names* and then click **Create Stack**.
 5. Wait until the Stack creation is complete. You can click on the **Refresh** button to track progress.
 6. Navigate to the **Outputs** tab and copy the Value that corresponds with the **TenableRoleArn** key.
 7. Paste the IAM Role ARN in the wizard and then click **Next**.
- **CloudFormation (AWS CLI):**
 - a. Open a new shell session with the latest version of the [AWS CLI](#). Administrator privileges are required to create the CloudFormation stack
 - b. Copy the command that appears in step B of the wizard, and run it in your shell. The following is a command example, but be aware that the parameters and values may differ depending on the permissions you selected.

Bash	Copy
<pre>aws cloudformation create-stack --stack-name TenableStack --template-url https://tenable-utilities.s3.us-east-2.amazonaws.com/Onboarding/AWS/CloudFormation/Template.json -- capabilities CAPABILITY_NAMED_IAM --parameters ParameterKey=RoleName,ParameterValue=TenableRole ParameterKey=RoleExternalId,ParameterValue=ba2edce3-d9e1-4ae4-8b33-ecd3961aed8c ParameterKey=RoleTrustedPrincipalId,ParameterValue=789846361812 ParameterKey=RoleMonitoringPolicy,ParameterValue=true ParameterKey=RoleRemediationPolicy,ParameterValue=false ParameterKey=RoleJitPolicy,ParameterValue=false ParameterKey=RoleWorkloadProtectionPolicy,ParameterValue=true ParameterKey=CloudTrailBucketName,ParameterValue=- ParameterKey=CloudTrailKeyArn,ParameterValue=-;aws cloudformation wait stack-create-complete --stack-name TenableStack;aws cloudformation describe-stacks --stack-name TenableStack --query "Stacks[0].Outputs"</pre>	

- c. After completing stack creation, copy the **OutputValue** that corresponds with the **TenableRoleArn** key from the shell.
- d. Paste the **IAM Role ARN** in the wizard and then click **Next**.

- o **Manual (AWS Console):**

- a. In the AWS Management Console, navigate to **IAM > Roles** and click **Create role**.
- b. For the trusted entity type, select **AWS account**.
- c. For the AWS account, select **Another AWS account** and then enter one of the following numbers as the Account ID, depending on your AWS environment type, and reflecting the value that appears in Step 1 of the wizard:

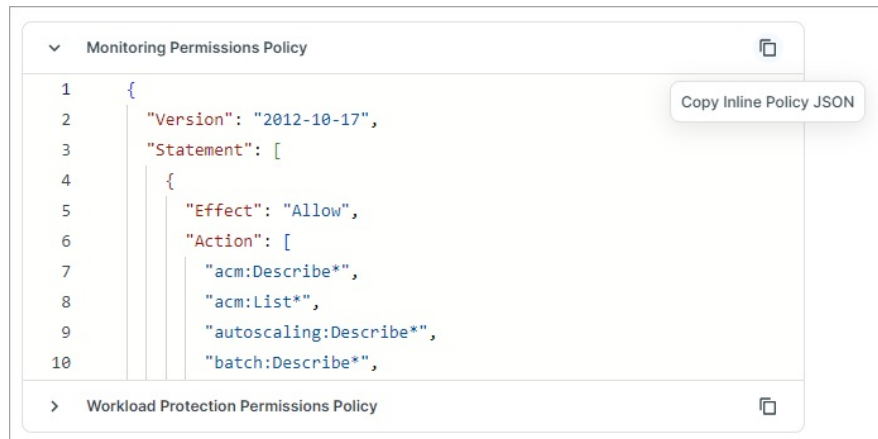
- Public Cloud: 081802104111
- US Gov Cloud: 757023926892

This is Tenable's account ID. The ID must be exactly twelve-digits; make sure not to include any extra spaces.

- d. Under Options, check **Require external ID**.
- e. Enter the Role External ID provided in step 3 of the Add Account wizard.

The Role External ID is a unique identifier that Tenable Cloud Security assigns to your customer account. This ID will be the same for each account you create for your organization. For more information, refer to <https://docs.aws.amazon.com/IAM/latest/UserGuide/co nfused-deputy.html>.

- f. In the list of policies, search for and select the **SecurityAudit permissions** policy and then finish creating the role. See [Required Permissions](#) to learn more about why Tenable needs these permissions granted.
- g. Open the newly created role and click **Add inline policy** in the permissions tab.
- h. Open the newly created role.
- i. For each of the policies that appear in step 3 (*IAM Role*) of the wizard in the Tenable Cloud Security Console, perform the following to create an inline policy:
 1. Click **Add permissions > Create inline policy**.
 2. Copy the policy that appears in the wizard and paste it in the JSON editor. For example:



3. Click **Next** and then finish creating the policy.

j. Paste the IAM Role **ARN** in the wizard and then click **Next**.

5. **Select a CloudTrail.** Select a CloudTrail for management events (required) and [S3/Lambda data events](#) (Step 5 in wizard). See [CloudTrail Logs](#) for important information and best practices related to granting Tenable access to trails.

a. Under **Management events**, select a primary CloudTrail with management events enabled for Tenable Cloud Security to read activity logs from:

Only valid trails are displayed here. For more information, see [CloudTrail Logs](#).

- If you use a single CloudTrail with both management events AND data events (either S3, Lambda, or both) enabled, select that trail from the dropdown. The **S3 Data events** and/or **Lambda Data events** field will be automatically populated with the CloudTrail information that you select here.
 - If you use separate trails for management events and data events (either S3, Lambda, or both), select the CloudTrail with management events enabled here, and the data event trail/s in the respective field.
- b. (Optional) Under **S3 Data events** and/or **Lambda Data events**, select the relevant CloudTrail. See [Enable Granular Recommendations Based on Data Events](#) for more information.

- c. If you haven't yet granted permissions to the S3 bucket where the trail logs are stored, follow the on-screen instructions to do so.
- d. If the KMS key for the CloudTrail is located in a different AWS account than the one that contains the S3 bucket, you need to [grant Tenable Cloud Security access to the key](#).

6. Click **Finish**.

After your account is added successfully, the account appears in the table in **Accounts > AWS**. Data about resources in your account will start to appear in Tenable Cloud Security. The time it takes for all data to appear varies depending on the size of your cloud environment. See [Manage Your Accounts in Tenable](#) for more information.

Onboard an AWS China Account

Onboard individual AWS China accounts to Tenable Cloud Security. When you onboard your account, Tenable Cloud Security doesn't copy any data from your account. Tenable only copies configuration metadata and CloudTrail event logs (optional). This information is saved in the region where you deployed Tenable Cloud Security.

- Onboarding is available for individual accounts only, and not organizations.
- AWS China accounts support the following features and functionality:
 - CIEM/CSPM
 - [Data Protection via onsite scanning](#) (Enterprise license)
 - [Workload Protection via onsite scanning](#) (Enterprise license)
- Tenable does not deploy servers in AWS China. Instead, asset configurations (and optionally, event logs) are copied from AWS China to another region in which Tenable [is deployed](#) (for example, the United States). This data is then stored alongside data synchronized from any of your non-China accounts.

To onboard an AWS China account:

1. Create an IAM user:

- a. In the AWS Management Console for one of your China accounts, navigate to **IAM > Users**.

If you have more than one China account, you can create the user in any of your accounts. It doesn't matter which one.

- b. Click **Create user**.
- c. Enter a meaningful **User name**.
- d. Verify that the *Provide user access to the AWS Management Console* checkbox is **not** selected.
- e. Click **Next**.
- f. On the *Set permissions* page, click **Next** without making any configuration changes.
- g. Review the user details and then click **Create user**.

2. Add an inline policy:

- a. Find and click on the user you just created in the Users table.
- b. Under Permissions, click **Add permissions > Create inline policy**.
- c. In the Policy editor, click **JSON**, and then paste the following code into the editor:

JSON	Copy
<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws-cn:iam::*:role/tenable-cs-role" }] }</pre>	

- `tenable-cs-role` is used as the role name in the above policy, but you can change the name if needed.
- Save this role name (default: `tenable-cs-role`), since you will need it later during account onboarding.

d. Click **Next**.

e. Enter a meaningful **Policy name** and then click **Create policy**.

3. Create an access key:

You can create a single access key for multiple accounts. There is no need to repeat this step for each additional account.

- For the user you created, under Security credentials, click **Create access key**.
 - Select **Third-party service** and then click **Next** (select the checkbox to confirm).
 - Click **Create access key**.
 - On the Retrieve access keys page, securely save the **Access key** and **Secret access key** values and then click **Done**.
- [Contact Technical Support](#) and securely provide them with the access key and secret for the IAM role you created.
 - With this information, Support will then enable AWS China to be used as a partition during account onboarding.
 - [Onboard your AWS China account](#), keeping in mind the following:
 - In step 1 of the onboarding wizard, under *AWS Partition*, select **China**.
 - In step 3 of the onboarding wizard, ensure that the IAM role you create is given the same name as the role in the policy you created earlier (default: `tenable-cs-role`).

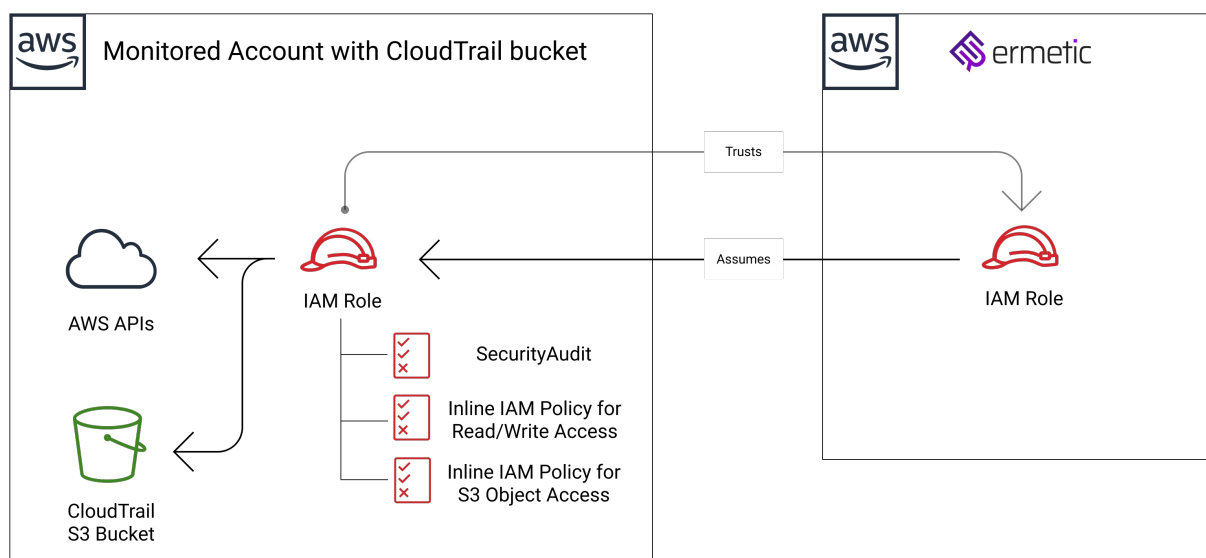
Account Architecture

Accounts With Monitoring/Remediation Permissions

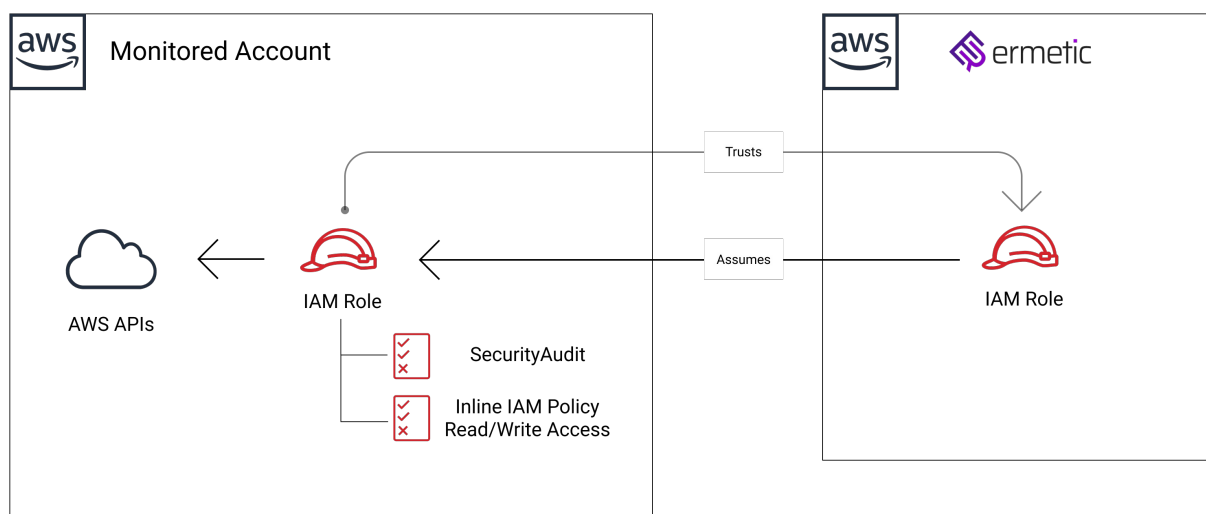
The following diagrams outline the architecture for accounts with Monitoring/Remediation [permissions](#), highlighting the differences between accounts that are connected to a CloudTrail and those that aren't. See [Cloud Trail Logs](#) for more information.

These diagrams show the trust relationship established between the IAM role associated with the account you onboard, and Tenable Cloud Security, which uses its own IAM role to interact with and collect data from your environment via [granted permissions](#).

CloudTrail Connected



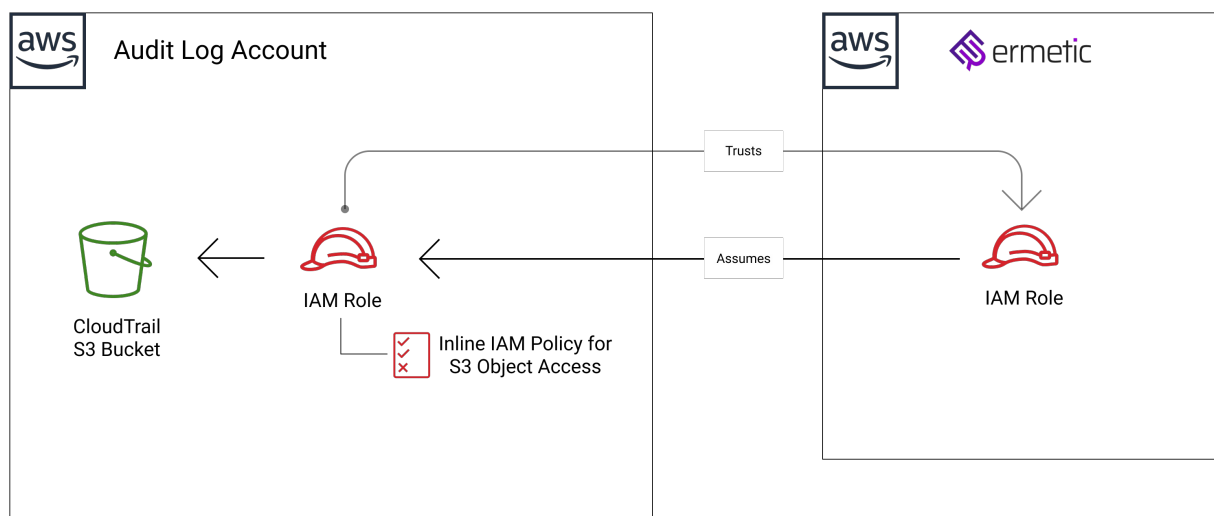
No CloudTrail Connected



Accounts With CloudTrail Permissions

This diagram shows the trust relationship established between the IAM role associated with the account you onboard, and Tenable Cloud Security, which uses its own IAM role to interact with and collect data from your

An *audit log account* is an account where only **CloudTrail** permissions were enabled/granted, without **Monitoring** permissions. Such an account is dedicated to collecting activity logs and will not be monitored for security purposes. Although Tenable Cloud Security supports onboarding accounts in such a way, it is recommended to onboard all accounts with **Monitoring** permissions, to provide full security visibility for your cloud assets.



Required Permissions

To provide full visibility into your account, Tenable Cloud Security needs to collect relevant metadata using both an AWS-managed policy and an inline policy that are attached to the dedicated role you create for Tenable in IAM when you [onboard an account](#):

- **Monitoring permissions:**
 - **SecurityAudit** permissions. AWS-managed policy, which grants access to read security configuration metadata.
 - Custom Tenable Monitoring permissions (read-only). [Inline policy](#), which grants Tenable additional read-only permissions not included in the SecurityAudit policy.

To learn more about why Tenable needs both the SecurityAudit policy and a custom, inline policy, see [Frequently Asked Questions](#).

- (Optional) Custom Tenable **Remediation** permissions (read-write). [Inline policy](#), which grants Tenable management permissions, allowing Tenable to make changes in your environment. For example, this allows Tenable to automatically remediate findings directly in AWS (If you choose not to grant management permissions, you can still manually remediate findings by providing one-time credentials on demand).
- **CloudTrail (S3)** permissions. See [CloudTrail Logs](#) for more information.

If you use service control policies (SCPs) in your AWS organization, make sure to add exclusions to any existing SCP to ensure that the dedicated IAM role you create for Tenable Cloud Security is not included. See [Frequently Asked Questions](#) for more information.

CloudTrail Logs

As part of the monitoring process, Tenable Cloud Security needs to read data from a CloudTrail that logs activity for the onboarded account. During the account onboarding process, you must choose a trail to use, and then grant Tenable access to the S3 bucket where the trail is located via an IAM role. Follow the guidelines in the [account](#) and [organization](#) onboarding steps.

During onboarding, Tenable identifies and displays a list of valid trails that are:

- **Multi-region.** See [Frequently Asked Questions](#) for more information about why a multi-region trail is needed.
- **Configured to log management read and write events.**
- **Enabled for logging.**

Each onboarded account generally has one associated CloudTrail, but there may be accounts with two or more trails.

If the S3 bucket where the CloudTrail files are stored is not in the same account as the account that you're onboarding, you need to independently [onboard](#) that account as well before you can choose it as a CloudTrail for the other account. If you use a separate AWS account as a “log archive account” to log activity for other accounts, Tenable recommends following this best practice:

- Onboard log archive accounts with both **Monitoring AND CloudTrail** permissions, to provide full visibility into all of your AWS accounts. If, however, for some reason you don't want Tenable Cloud Security to scan such accounts for security monitoring, you can onboard it with **CloudTrail** permissions only.

Benefits of Granting CloudTrail Access

It is recommended to always grant Tenable access to the S3 bucket containing your CloudTrail when onboarding accounts. Doing so provides several important benefits, including:

- *Cloud Detection and Response:*
 - Visibility into activity performed by identities within your cloud environment ([Activity Log](#)).
 - Continuous risk analysis that checks for anomalies against behavioral baselines ([Anomaly Detection](#)).
- Visibility into effective use of permissions based on activity (used permissions).
- Fine-grained least-privilege recommendations based on usage. See [Enable Granular Recommendations Based on Data Events](#) for details.

Enable Granular Recommendations Based on Data Events

To enable action- and resource-granular recommendations within Tenable Cloud Security, enable [CloudTrail data read/write event logging](#) for S3 buckets/objects and Lambda functions, and then select the relevant trail/s in Tenable Cloud Security.

This ensures that, in addition to viewing generic information about access to a given AWS service, you can also analyze much more valuable information about:

- when a given identity used a specific action in the service
- exactly which resource within the service the identity used

In turn, this allows Tenable Cloud Security to provide specific, least-privilege recommendations related to this data. For example, Tenable can provide least-privilege recommendations down to the specific S3 bucket used by an application.

You can configure Tenable Cloud Security to work with your CloudTrail in one of the following ways, depending on whether you have data events enabled:

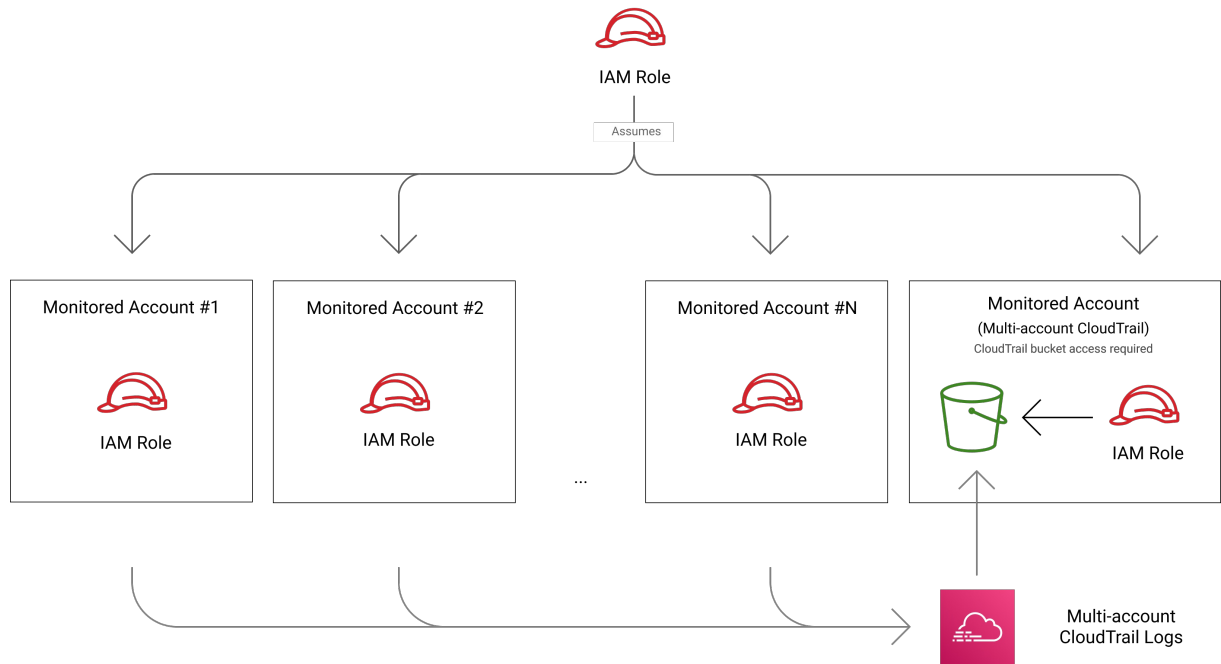
- If you use a single CloudTrail with both management events AND data events (either S3, Lambda, or both) enabled, select that trail from the **Management events** dropdown. The **S3 Data events** and/or **Lambda Data events** field will be automatically populated with the CloudTrail information that you select here.
- If you use separate trails for management events and data events (either S3, Lambda, or both), select the CloudTrail with management events enabled from the **Management events** dropdown, and the data event trail/s in the respective field.

CloudTrail Deployment

The following diagrams show how CloudTrail can be deployed in environments with multiple accounts, highlighting the differences between environments that maintain a dedicated CloudTrail (*organizational trail*) for multiple accounts, and those that have individual CloudTrails for each account.

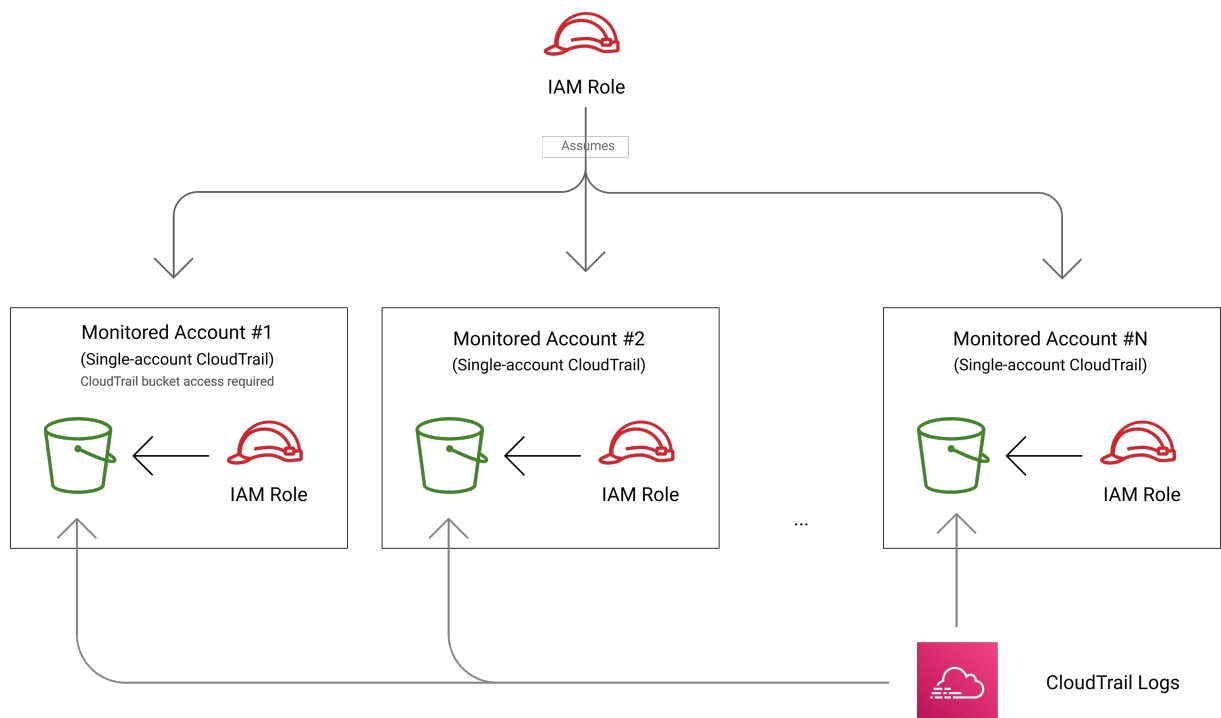
Dedicated Organization Trail for Multiple Accounts

In this scenario, a separate, dedicated AWS account is used as a *log archive account*, containing an organizational trail which logs activity for other accounts. This dedicated account should be independently onboarded to Tenable Cloud Security with Monitoring permissions, and its organizational trail can then be used as the shared CloudTrail for other accounts that you onboard to Tenable. If you are onboarding an entire organization, complete organization onboarding, and then edit the relevant account and grant Tenable CloudTrail permissions via the IAM role.



Single CloudTrail Bucket per Account

In this scenario, each onboarded account connects to an independent CloudTrail (identically named across accounts).



KMS Key in Different Account

If the KMS key for the CloudTrail is located in a different AWS account than the one you're currently adding, you need to grant Tenable Cloud Security access to the key.

To grant access to a KMS key located in a different account:

1. Navigate to the AWS account where the CloudTrail KMS key is located.
2. Navigate to **KMS > Customer managed keys** and open the relevant KMS key.
3. **Edit** the key policy and add the following statement to the "Statement" section:

JSON	Copy
<pre>{ "Sid": "Allow an external account to use this KMS key", "Effect": "Allow", "Principal": { "AWS": "{ErmeticRoleARN}" }, "Action": "kms:Decrypt", "Resource": "*" }</pre>	

Where `ErmeticRoleARN` is the Role ARN of the role you created earlier in this wizard.

4. Click **Save Changes**.

Account Status and Troubleshooting

Tenable Cloud Security displays a **Status** for each account on the **Accounts > AWS** page, indicating, for example, whether Tenable can connect to the account, and helping you troubleshoot potential onboarding issues.

Status	Description
Access denied	Tenable Cloud Security wasn't able to synchronize one or more resource types. Although there are various reasons why this might happen, it is likely because you need to update the Tenable Cloud Security read-only policy (added during account onboarding) in AWS.

Account not found	
Connected	Tenable Cloud Security successfully connected to the account, and the account is up and running.
Connected with issues	<p>The cluster is connected, but there are specific issues that need to be addressed:</p> <ul style="list-style-type: none"> • JIT permissions not granted • Private S3 bucket scanning permissions (Data Protection) not granted • EC2 Instance scanning permissions (Workload Protection) not granted • ECR scanning permissions (Workload Protection) not granted • Terraform (S3) permissions not granted • Missing permissions required for reading events
Deleting... this may take up to an hour	You deleted the account in Tenable Cloud Security, and the process hasn't completed yet.
Disconnected	There is an issue with the IAM role that you created during account onboarding to delegate permissions to Tenable Cloud Security. It may have been deleted, or there was a change in the trust policy that prevents Tenable from assuming the role.
Invalid permissions	There is an issue with the IAM role that you created during account onboarding to delegate permissions to Tenable Cloud Security. Some permissions are missing. Please add the required permissions to the IAM role.
Failed to query regions	Tenable Cloud Security was unable to query the active regions that you selected in account onboarding. One or more of the regions may be disabled. Please modify the region list or add an exclusion for the IAM Role from your SCPs. Refer to the relevant AWS documentation for more information.
Pending deletion	The account is pending closure in AWS. It will eventually be deleted. Resources and findings associated with accounts pending deletion are hidden in Tenable Cloud Security.
Read-only policy is incorrect	<p>The Tenable Cloud Security read-only policy is missing one or more of the following actions:</p> <ul style="list-style-type: none"> • <code>AwsCloudTrail.Actions.DescribeTrails</code> • <code>AwsCloudTrail.Actions.GetEventSelectors</code> • <code>AwsCloudTrail.Actions.GetTrail</code> • <code>AwsCloudTrail.Actions.GetTrailStatus</code>

Suspended	The account is suspended in AWS. It will eventually be deleted. Resources and findings of suspended accounts are hidden in Tenable Cloud Security.
------------------	--

CloudTrail Status

See [CloudTrail Logs](#) for more information about CloudTrail-related issues.

Status	Description
Connected	Analyzing CloudTrail logs
Duplicate events	CloudTrail contains duplicate events. Please ensure the trail is configured correctly. This can happen if you configure multiple trails for the same account that cover overlapping event types.
Invalid CloudTrail configured	Invalid CloudTrail configured. Please select a valid trail or modify its configuration.
Missing permissions	Missing permissions to the CloudTrail service (cannot fetch list of trails).
Missing permissions to bucket	Missing permissions to read CloudTrail events from the target S3 bucket (may belong to a different account).
Not configured	CloudTrail logs aren't being analyzed. Please configure a valid trail.

Appendix I: AWS IAM Policies

- [Tenable Monitoring Policy \(Read-only\)](#)
- [Tenable Remediation Policy \(Read-write\)](#)
- [CloudTrail Policy](#)
- [EC2 Instance Scanning Workload Protection Policy](#)
- [ECR Scanning Workload Protection Policy](#)
- [Terraform Policy](#)
- [JIT Policy](#)

Tenable Monitoring Policy (Read-Only)

JSON	Copy
<pre>{ "Version": "2012-10-17", "Statement": [{</pre>	

```
"Effect": "Allow",
"Action": [
    "acm:Describe*",
    "acm:List*",
    "autoscaling:Describe*",
    "batch:Describe*",
    "batch:List*",
    "bedrock:Get*",
    "bedrock:List*",
    "cloudformation:Describe*",
    "cloudformation:Get*",
    "cloudformation:List*",
    "cloudfront:Get*",
    "cloudfront:ListDistributions*",
    "cloudtrail:Describe*",
    "cloudtrail:Get*",
    "cloudtrail:List*",
    "cloudtrail:LookupEvents",
    "cloudwatch:Describe*",
    "cloudwatch:GetMetric*",
    "cloudwatch:ListMetrics",
    "cognito-idp:ListResourcesForWebACL",
    "cognito-sync:GetCognitoEvents",
    "config:Describe*",
    "dynamodb:Describe*",
    "dynamodb:List*",
    "ec2:Describe*",
    "ecr:Describe*",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:GetRepositoryPolicy",
    "ecr:List*",
    "ecr:StartImageScan",
    "ecr-public:Describe*",
    "ecr-public:GetRepositoryPolicy",
    "ecr-public:List*",
    "ecs:Describe*",
    "ecs:List*",
    "eks:Describe*",
    "eks:List*",
    "elasticache:Describe*",
    "elasticache:List*",
    "elasticbeanstalk:Describe*",
    "elasticbeanstalk:List*",
    "elasticloadbalancing:Describe*",
    "elasticmapreduce:Describe*",
```

```
"elasticmapreduce:List*",
"es:Describe*",
"es:List*",
"events:ListRules",
"iam:Generate*",
"iam:Get*",
"iam:List*",
"identitystore:Describe*",
"inspector2:List*",
"iot:GetTopicRule",
"kms:Describe*",
"kms:GetKey*",
"kms:List*",
"kinesis:Describe*",
"kinesis:List*",
"lambda:Get*Policy",
"lambda:GetAccountSettings",
"lambda:List*",
"logs:Describe*",
"organizations:Describe*",
"organizations:List*",
"rds:Describe*",
"rds:List*",
"redshift:Describe*",
"redshift:List*",
"route53:Get*",
"route53:List*",
"route53domains:Get*",
"route53domains:List*",
"route53resolver:Get*",
"route53resolver:List*",
"s3:Describe*",
"s3:GetAccessPoint*",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetJobTagging",
"s3:GetLifecycleConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListBucketVersions",
"s3:ListJobs",
"secretsmanager:Describe*",
"secretsmanager:GetResourcePolicy",
"secretsmanager:List*",
```

```

        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "ssm:Describe*",
        "ssm:List*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sts:DecodeAuthorizationMessage",
        "tag:Get*",
        "wafv2:Get*",
        "wafv2:List*"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::elasticbeanstalk-*"
},
{
    "Effect": "Allow",
    "Action": "apigateway:Get*",
    "NotResource": "arn:aws:apigateway:*::/apikeys*"
}
]
}

```

Tenable Remediation Policy (Read-Write)

JSON	Copy
<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", </pre>	

```
"Action": [  
  "ec2:DeleteSecurityGroup",  
  "ec2:ModifyInstanceMetadataOptions",  
  "ec2:ModifyVpcEndpoint",  
  "ec2:RevokeSecurityGroupEgress",  
  "ec2:RevokeSecurityGroupIngress",  
  "ecr:DeleteRepositoryPolicy",  
  "ecr:SetRepositoryPolicy",  
  "iam:AddUserToGroup",  
  "iam:AttachGroupPolicy",  
  "iam:AttachRolePolicy",  
  "iam:AttachUserPolicy",  
  "iam:CreatePolicy",  
  "iam:CreatePolicyVersion",  
  "iam:DeactivateMFADevice",  
  "iam:DeleteAccessKey",  
  "iam:DeleteGroup",  
  "iam:DeleteGroupPolicy",  
  "iam:DeleteLoginProfile",  
  "iam:DeletePolicy",  
  "iam:DeletePolicyVersion",  
  "iam:DeleteRole",  
  "iam:DeleteRolePermissionsBoundary",  
  "iam:DeleteRolePolicy",  
  "iam:DeleteServerCertificate",  
  "iam:DeleteServiceSpecificCredential",  
  "iam:DeleteSigningCertificate",  
  "iam:DeleteSSHPublicKey",  
  "iam:DeleteUser",  
  "iam:DeleteUserPermissionsBoundary",  
  "iam:DeleteUserPolicy",  
  "iam:DetachGroupPolicy",  
  "iam:DetachRolePolicy",  
  "iam:DetachUserPolicy",  
  "iam:PutGroupPolicy",  
  "iam:PutRolePermissionsBoundary",  
  "iam:PutRolePolicy",  
  "iam:PutUserPermissionsBoundary",  
  "iam:PutUserPolicy",  
  "iam:RemoveRoleFromInstanceProfile",  
  "iam:RemoveUserFromGroup",  
  "iam:UpdateAccessKey",  
  "iam:UpdateAssumeRolePolicy",  
  "s3:DeleteBucketPolicy",  
  "s3:PutBucketPolicy",
```

```

        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "sso:DeleteAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet"
    ],
    "Resource": "*"
}
]
}

```

CloudTrail Policy

JSON	Copy
<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:GetBucketLocation", "s3:GetObject", "s3:ListBucket"], "Resource": ["arn:aws:s3:::ttt", "arn:aws:s3:::ttt/*"] }] } </pre>	

Private S3 Bucket Scanning Data Protection Policy

JSON	Copy
<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:GetObject", "s3:ListBucket"], "Resource": "*" }] }</pre>	

EC2 Instance Scanning Workload Protection Policy

JSON	Copy
<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "ec2:CreateSnapshot", "Resource": "arn:aws:ec2:*:*:volume/*" }, { "Effect": "Allow", "Action": "kms:CreateAlias", "Resource": "arn:aws:kms:*:*:alias/*" }, { "Effect": "Allow", "Action": ["ec2:CopySnapshot", "ec2:CreateSnapshot", "ec2:CreateTags", "kms:CreateKey", "kms:TagResource"], "Resource": "*" }] }</pre>	

```

    "Condition": {
      "StringEquals": {
        "aws:RequestTag/ErmeticContext": "WorkloadAnalysis"
      }
    },
    {
      "Effect": "Deny",
      "Action": "kms:TagResource",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/ErmeticContext": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "kms:CreateAlias",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:EnableKeyRotation",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:ReEncryptFrom"

```

```

    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "ec2.*.amazonaws.com"
      }
    }
  }
]
}

```

ECR Scanning Workload Protection Policy

JSON	Copy
<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["ecr:GetAuthorizationToken", "ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage"], "Resource": "*" }] } </pre>	

Terraform Policy

JSON	Copy
<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:GetBucketLocation", "s3:GetObject", "s3:ListBucket"], "Resource": ["arn:aws:s3:::<bucket_name>", "arn:aws:s3:::<bucket_name>/*",] }] } </pre>	

Where `<bucket_name>` is the name of the relevant S3 bucket.

JIT Policy

If you're using a delegated administrator account, make sure to grant `{{variable.Product_name}}` permissions in the delegated account, and not the management account, using the [JIT policy for delegated administrator account](#).

JSON	Copy
<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:ListRoles", "iam:ListPolicies"], "Resource": "*" }, { "Effect": "Allow", </pre>	

```

        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam>DeleteRole",
            "iam:GetRole",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/aws-
reserved/sso.amazonaws.com/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:GetSAMLProvider",
            "iam:UpdateSAMLProvider"
        ],
        "Resource": "arn:aws:iam::*:saml-
provider/AWSSSO_*_DO_NOT_DELETE"
    },
    {
        "Effect": "Allow",
        "Action": [
            "sso:AttachManagedPolicyToPermissionSet",
            "sso:CreateAccountAssignment",
            "sso:CreatePermissionSet",
            "sso>DeleteAccountAssignment",
            "sso>DeletePermissionSet",
            "sso:Describe*",
            "sso:DetachManagedPolicyFromPermissionSet",
            "sso:Get*",
            "sso:List*",
            "sso:ProvisionPermissionSet",
            "sso:PutInlinePolicyToPermissionSet",
            "sso-directory:List*",
            "sso-directory:Search*"
        ],
        "Resource": "*"
    }
]
}

```

JIT Policy for Delegated Administrator Account

If you're using a delegated administrator account, make sure to grant {{variable.Product_name}} permissions in the delegated account, and not the management account.

JSON	Copy
<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["sso:AttachManagedPolicyToPermissionSet", "sso:CreateAccountAssignment", "sso:CreatePermissionSet", "sso>DeleteAccountAssignment", "sso>DeletePermissionSet", "sso:DetachManagedPolicyFromPermissionSet", "sso:ProvisionPermissionSet", "sso:PutInlinePolicyToPermissionSet"], "Resource": "*" }] }</pre>	