Implementation Guide:

Prisma Cloud – AWS Control Tower Implementation
## Table of Contents

Foreword ...................................................................................................................................... 3
Solution overview and features .................................................................................................... 4
Prisma Cloud AWS Control Tower Architecture ............................................................................ 4
Pre-requisites ................................................................................................................................ 6
Best Practices .................................................................................................................................. 13
Solution Estimated Pricing .......................................................................................................... 13
Additional resources ................................................................................................................... 13
Foreword

The Prisma™ Cloud is a security and compliance service that dynamically discovers cloud resource changes and continuously correlates raw, siloed data sources, including user activity, resource configurations, network traffic, threat intelligence, and vulnerability feeds, to provide a complete view of cloud risk. Through an innovative, machine learning-driven approach, Prisma Cloud enables organizations to quickly prioritize risks, maintain agile development, and effectively fulfill their obligations in the shared responsibility model.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Prisma™ Cloud in 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

Prisma Cloud unifies Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) into a single cloud native security platform. Continuously monitor your environment and immediately enforce governance with hundreds of pre-built policies. Prisma Cloud ingests all major AWS APIs and sources threat intelligence from over 30 feeds including AutoFocus to provide comprehensive visibility. Risk-ranked alerts prevent remediation fatigue and 1-click compliance reporting eases auditing across even the most complex distributed environments. Prisma Cloud also provides full lifecycle security for any cloud native workload or application. It protects applications and the underlying compute resources including containers and functions by integrating security into AWS CodeDeploy and Elastic Container Registry (ECR) while protecting running workloads and apps. Through this integrated approach only Prisma Cloud enables SecOps and DevOps to stay agile, collaborate effectively and securely accelerate cloud native application development and deployment across their entire AWS environment.

Benefits of Prisma Cloud on AWS

- Visualize every connected resource across your AWS environment.
- Maintain continuous compliance and easily generate reports across your AWS environment.
- Enable secure DevOps by setting guardrails with real time monitoring for threats, such as risky configurations, sensitive user activities, network intrusions, and host vulnerabilities.
- Use anomaly detection capabilities to root out account compromises and insider threats.
- Investigate current threats or past incidents and quickly determine root causes.
- Get contextual alerts to help your team prioritize issues and respond quickly.

Prisma Cloud AWS Control Tower Architecture

With consolidated access to AWS services and resources across your company within AWS Organizations, you can onboard the AWS master account on Prisma Cloud. When enabling the AWS Organizations on the AWS management console and adding the root or master account that has the role of a payer account that is responsible for paying all charges accrued by the accounts in its organization, all member accounts within the hierarchy are added in one streamlined operation on Prisma Cloud. As a part of the AWS Control Tower execution first deploy/trigger a CloudFormation template in the master account as a part of the workflow to create the Prisma Cloud role to monitor or monitor and protect your resources deployed on the master account and leverage CloudFormation StackSets to automate the creation of the Prisma Cloud role, which authorizes
Prisma Cloud to access each member account. When a new member account is added to your AWS organization, it is onboarded automatically on Prisma Cloud. Additionally, as a part of the Control Tower execution trigger CloudFormation StackSet to allow Lambda Serverless remediation functions to make necessary changes in the master and member accounts.

![Diagram](image)

**Figure 1: Prisma Cloud governance on AWS Organization Account: Read Only/ Read Write**

(The above Figure shows how a new Member Account will be onboarded to Prisma Cloud with either ReadOnly or ReadWrite Mode automatically once provisioned from AWS Control Tower Environment).
Prisma Cloud also integrates with Amazon GuardDuty, AWS Inspector and AWS Security Hub. Prisma Cloud starts ingesting GuardDuty data, correlates it with the other information that Prisma Cloud already collects, and presents contextualized and actionable information through the Prisma Cloud app, it also ingests vulnerability data and security best practices deviations from AWS Inspector to provide organizations with additional context about risks in the cloud and you can also integrate Prisma Cloud with AWS Security Hub for centralized visibility into security and compliance risks associated with your cloud assets on the AWS Security Hub console.

Pre-requisites

- Subscribe to Prisma Cloud on AWS Marketplace
- If you are new to AWS, see Getting Started with AWS (https://aws.amazon.com/getting-started/)
- For additional information on AWS Marketplace, see
To get started with AWS Control Tower, check out the [Deployment and Configuration Steps](https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html)

**Deployment and Configuration Steps**

**Step 1:** Subscribe to Prisma Cloud on AWS Marketplace.


Click on the **Continue to Subscribe** button.

**Step 2:** Deploy Relevant Cloudformation templates:

Select the Mode. Decide whether to enable permissions to only monitor (read-only access) or to monitor and protect (read-write access) the resources in your cloud account. Your selection determines which AWS CloudFormation Template (CFT) is used to automate the process of creating the custom role required for Prisma Cloud.

Login to Master Account, select **Services, CloudFormation, CreateStack**, upload one of the below templates as per the deployment mode you choose.

**Monitor mode:** [https://s3.amazonaws.com/redlock-public/cft/rl-read-only.template](https://s3.amazonaws.com/redlock-public/cft/rl-read-only.template)


- **Stack Name** — The default name for the stack is **PrismaCloudApp**.
• **ExternalID** — The Prisma Cloud ID, a randomly generated UUID that is used to enable the trust relationship in the role's trust policy. Provide a random value like the example shown in template (Ex: - “PrismacloudAWSTest22453”). You will feed in this external-id in Prisma Cloud portal in step-6.

• **PrismaCloudRoleName** — The name of the role that will be used by Prisma Cloud to authenticate and access the resources in your AWS account, or keep the default Role provided in template.

**Step 3:** Accept the IAM acknowledgment for resource creation and select **Create Stack**. The stack creation is initiated. Wait for the **CREATE_COMPLETE** status.

**Step 4:** Select **Outputs** and copy the value of the **PrismaCloudARN**. This will be used in step-6. The Prisma Cloud Role has the permissions required for enabling authentication between Prisma Cloud and your AWS account.

**Step 5:** Create a StackSet to create the Prisma Cloud role within each member account. AWS StackSets enables you to automate the process of creating the Prisma Cloud role across multiple accounts in a single operation.

5.a Download the template file.

• For member accounts with read-only access permissions (Monitor mode)- https://s3.amazonaws.com/redlock-public/cft/rl-read-only-member.template

• For member accounts with the read-write access permissions (Monitor & Protect mode)- https://s3.amazonaws.com/redlock-public/cft/rl-read-and-write-member.template

5.b Log in to AWS management account, and choose **Services, CloudFormation, StackSets, Create StackSet**.

5.c Upload the template file and click **Next**, then enter a StackSet Name.

5.d In Parameters, enter the values for **PrismaCloudRoleName** and **ExternalId**.

   Note: The PrismaCloudRoleName must include **Org** within the string, Both Rolename and ExternalId will be used at later step.

   • Example RoleName – “PrismaCloudOrgMemberReadOnlyRole”
   • Example ExternalID – “PrismacloudAWSTestMemberAccount12345”)

5.e Click **Next** and select **Service managed permissions**

5.f Click **Next** and select **Deploy to organization** under Deployment targets.

If you do not want to onboard all member accounts, you can select **Deploy to organization unit OUs** and deploy the Stackset only to selected OUs only.
5.g Set Automatic deployment **Enabled**, and Account removal behavior **Delete stacks**.

5.h Under Specify regions, select one region. Recommended to keep it same as AWS Control Tower home region.

5.i For Deployment Options, Maximum concurrent accounts, select **Percentage** and set it to **100**.

5.j For Deployment Options, Failure tolerance, select **Percentage** and set it to **100**.

5.k Click **Next**, and review the configuration.

5.l Select I **acknowledge that AWS CloudFormation might create IAM resources with custom names** and **Submit**

The StackSet creation is initiated. Wait for the SUCCEEDED status. When the process completes, each member account where the role was created is listed under Stack **instances** on the AWS management console.

**Step 6: Add a New AWS Organization Account on Prisma Cloud**

6.a Login to Prisma Cloud, Select Settings, Cloud Accounts, Add New and select AWS as the Cloud to Protect.

Note: When Subscribed to marketplace in step-1, You will receive a welcome email from Palo Alto Networks (**noreply@prismacloud.paloaltonetworks.com**) that includes a link to where you can access your instance of Prisma Cloud.

6.b Enter a Cloud Account Name and onboard Organization.

- Log into Prisma Cloud and select **Settings, Cloud Accounts, Add New**.
- A cloud account name is auto-populated for you. You can replace it with a cloud account name that uniquely identifies your AWS Organization on Prisma™ Cloud.
- Select the Mode you have choosen in earlier steps for stack deployments.
6.c Configure the master account role details and click **Next**. (Please use the details copied earlier from step-2b and Step-4).

6.d Configure the member account role details and click **Next**.

Use the details you copied from the previous step to set up the trust relationship and retrieve data from the member accounts. (Please use the details copied earlier from step-5. d.)

**Note:** If you have a large number of member accounts, it may take a while to create the role in each account and list it for verification. If you want to verify that the role was created in all accounts, do not select the checkbox. You can edit the cloud account settings later and onboard the member accounts. If you do not select the checkbox, only the master account will be onboarded to Prisma Cloud.

Select “I confirm the stackset has created Prisma roles in member accounts successfully” and click **Next**.
6.e Select an “accountgroup” and click Next. Refer to below link for more details on Account groups - https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-account-groups.html

During initial onboarding, you must assign all the member cloud accounts with the AWS Organization hierarchy to an account group.

Note: If you would like to selectively assign AWS member accounts to different account groups on Prisma Cloud, you can edit the cloud account settings later. We Create an Alert Rule to associate with that account group so that alerts are generated when a policy violation occurs.

6.f Select an account group and click Next.
Step 7: Review the onboarding Status of your AWS Organization on Prisma Cloud.

The status check verifies that VPC flow logs are enabled on at least 1 VPC in your master account, and audit events are available in at least one region on AWS CloudTrail. It also displays the number of member accounts that are provisioned with the Prisma Cloud role.

Review the info and Select Done.

Optional steps to enable remediation:

Step 11: Configure the SQS Integration to invoke Lambda based remediation

Prisma Cloud can integrate with an SQS queue in the Management Account to sends alert notifications. The SQS can then be used to invoke an AWS Lambda function which would trigger an appropriate run book script to remediate the alert(s).
Use Case Example

If Prisma Cloud finds an S3 bucket does have SSE Encryption turned on it can trigger a lambda based remediation runbook to enable SSE encryption settings:

- Use the following CFT Templates to create an IAM role for Lambda Based Remediation:  [https://github.com/PaloAltoNetworks/Prisma-Enhanced-Remediation/tree/master/AWS/templates](https://github.com/PaloAltoNetworks/Prisma-Enhanced-Remediation/tree/master/AWS/templates)
- The complete Lambda package and list of runbooks is available here:  [https://github.com/PaloAltoNetworks/Prisma-Enhanced-Remediation/tree/master/AWS/lambda_package](https://github.com/PaloAltoNetworks/Prisma-Enhanced-Remediation/tree/master/AWS/lambda_package)

Best Practices

- Follow the Prisma Cloud Administration Best Practices here:  [https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators.html](https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators.html)

Solution Estimated Pricing


Additional resources

- Partner contact information  [https://www.paloaltonetworks.com/company/contact-support](https://www.paloaltonetworks.com/company/contact-support)