Managing AWS with Cisco Security Cloud Control

Managing AWS with Cisco Security Cloud Control

Using Cisco Security Cloud Control to Manage AWS VPCs

Security Cloud Control provides a simplified management interface for your Amazon Web Services (AWS) Virtual Private Clouds (VPCs). You can manage your AWS VPCs and their components in the same interface you manage your other devices.

Use Security Cloud Control to perform these tasks:

- Onboard an AWS VPC
- View VPC Details
- Work with Security Groups
- Share AWS Objects with other Managed Device
- Monitor AWS Site-to-Site VPN Connections
- Monitoring Changes to AWS Devices
- Viewing AWS Site-to-Site VPN Tunnels

These are common AWS features that Security Cloud Control expects to support in the future:

- Showing the relationship of load balancers (elastic, network, and application load-balancers) to the security group.
- Showing the relationship of auto-scaling groups to a security group.

You cannot manage these aspects of security groups with Security Cloud Control:

- Creating Security Groups.
- Linking Security Groups to instances.

- Assigning Security Groups to load balancers.
- VPC peering.

Onboard AWS VPCs

Start by onboarding the AWS VPC using Security Cloud Control's onboarding wizard. See Onboard an AWS VPC for more information.

Note that if an AWS VPC contains tags, these tags are imported into Security Cloud Control when you onboard the device. Security Cloud Control represents the tags as **labels**. Unlike security cloud objects or rules, labels are not automatically synchronized to the AWS VPC. See Labels and Filtering for more information.

Handle AWS VPC login credentials and permissions through the Security Cloud Control console. Without the correct credentials or permissions, Security Cloud Control cannot communicate with the AWS VPC. See Update AWS VPC Connection Credentials and Changing Permissions for an IAM User for more information.

View AWS VPC Details

Once the AWS VPC has been onboarded, you can view the AWS VPC's ID, region, security groups, and the rules and objects assigned to those security groups.

Work with Security Groups

Security groups are a collection of rules that govern inbound and outbound network traffic to all the AWS instances, and other entities, associated with the security group. When you onboard an AWS VPC to Security Cloud Control, the security groups are stored in Security Cloud Control as security group objects.

Using Security Cloud Control you can perform these tasks:

- Create new rules in a security group.
- Check for changes, edit, and delete rules in a security group.

At this time, you cannot create new security groups in a VPC.

See these topics for more information:

- AWS VPC Security Groups and Instances
- Manage AWS VPC Security Groups Rules
- Sharing Objects Between AWS and other Managed Devices

Share Objects Between AWS and Other Managed Devices

Security Cloud Control supports the use of objects in rules. Objects are containers for values. For example, you could have a network object that contains the IP address of a resource and give it a meaningful name. Then you can use that object in access rules as part of the source or destination of the rule, rather than using the resource's literal IP address. You can also re-use that object in different rules. If you change the value of the object once, any rule that uses that object starts using the new value.

After onboarding an AWS VPC, Security Cloud Control translates AWS concepts into security group objects, as well as network objects, and service objects found in existing security group rules.

Network objects and service objects (sometimes referred to as port objects) can be shared between AWS VPCs and other devices you manage using Security Cloud Control. Security group objects are unique to AWS.

See Sharing Objects Between AWS and other Managed Devices for more information.

Monitor AWS Site-to-Site VPN Connections

AWS site-to-site VPN connects your AWS VPC to your enterprise network through a secure tunnel. See AWS Site-to-Site VPN Management for more information.

Monitoring Changes to AWS VPCs and AWS Security Groups

Change Log

The change log continuously captures configuration changes as they are made in Security Cloud Control. This single view includes changes across all supported devices and services. These are some of the features of the change log:

- Side-by-side comparison of changes made to device configuration.
- Plain-English labels for all change log entries.
- Records on-boarding and removal of devices.
- Detection of policy change conflicts occurring outside of Security Cloud Control.
- Answers who, what, and when during an incident investigation or troubleshooting.

Change Request Management

Change request management allows you to associate a change request and its business justification, opened in a third-party ticketing system, with an event in the Change Log. Use change request management to create a change request in Security Cloud Control, identify it with a unique name, enter a description of the change, and associate the change request with change log events. You can later search the Change Log for the change request name.

Support for Common Managerial Tasks

Security Cloud Control supports these common management tasks for AWS security groups:

- Bulk Deploy Device Configurations
- Read All Device Configurations
- Detecting Out-of-Band Changes
- Conflict Detection
- Resolve Configuration Conflicts