Configuring AWS EC2 Connectors with Cross-Account Role Authentication (ARN)

Document created by Hari Srinivasan (/discussions/s/profile/0052L000003olee) on Apr 24, 2018. Last modified by Hari Srinivasan (/discussions/s/profile/0052L000003olee) on Apr 27, 2018.

Description
Qualys EC2 Connector now supports cross-account role-based authentication to connect to AWS account. This allows you to grant Qualys access to your AWS account to list EC2 instances without requiring IAM User security credentials. With EC2 Connector you can inventory your AWS EC2 instances within the account by assuming the IAM role that you create in your AWS account.

Users who had EC2 connector created using IAM access keys/secret keys can now migrate to cross-account role-based authentication. It is a recommended approach by AWS. IAM access keys require periodic rotation. Cross-account role removes the overhead, there are no keys to manage henceforth.

What does AWS EC2 Connector collect?

AWS EC2 connector inventory the instances under an account. It also collects metadata for every instance like ImageId, Instance State, Size, VPC, Subnet, EC2 Tags,..
The connector does DESCRIBE (read as "read-only") API calls to AWS API endpoint for Instances, Images, and Interfaces under the account, to build a complete EC2 inventory of your account.

Highlights

New EC2 Connector Creation

- New EC2 Connector creation will support only cross-account role-based authentication.

Wiz - EXHIBIT 1124
Wiz, Inc. v. Orca Security Ltd.
IPR2024-01191

- You can use CloudFormation template to automate the EC2 connector creation. You can directly download the template from the connector creation UI.
- REST API updated to support create/update cross-account role based EC2 connector.
- Creation of multiple connectors for the same AWS account is not permitted.

Updates to Existing EC2 Connectors

- You can now upgrade existing EC2 connector from access keys to cross-account role-based authentication.
- Your existing EC2 connector based upon IAM access keys will continue to function. You can manage them using UI or API, this support will be discontinued after **180 days.**
- In case you have multiple EC2 connectors for same AWS account then you need to remove duplicate connector before you switch to cross-account role-based authentication.

How to go about planning

- You can start with one or two of your existing EC2 connector for transitioning from access keys to a cross-account role.
- Since new EC2 Connector creation will support only cross-account role-based authentication, it is important to communicate the change in authentication mechanism to the account owners if new account to be added in future.
- Upgrade remaining EC2 connector to a cross-account role. You can use CloudFormation template or API to automate it.
- For step-by-step instructions refer the Securing Amazon Web Services with Qualys (product user guide) (https://www.qualys.com/docs/qualys-securing-amazon-web-services.pdf)

Frequently Asked Questions

What is a cross-account role?

A cross-account IAM role is an IAM role that includes a trust policy that allows AWS identities in another AWS account to assume the role. It is a more secure way of granting programmatic access to your AWS accounts. IAM access keys require periodic rotation and can be shared or stolen. Cross-account role minimizes the overhead of rotation of keys.

What happens to my existing EC2 connectors created using IAM access keys?
Existing EC2 connectors will function as before. You can upgrade your existing EC2 connector from access keys to cross-account role-based authentication.

Do I need to upgrade all my existing EC2 connectors immediately?
We will continue to support access-key based EC2 connectors for 180 days. Ensure that you migrate the access-key based EC2 connectors to cross-account role-based authentication within 180 days.

How can I quickly set up EC2 connectors for my multiple AWS accounts?
You can use the CloudFormation template or REST APIs to automate the EC2 connector creation process for multiple AWS accounts.

Can I create two connectors for the same AWS account?
No. Only one connector per AWS account is permitted.

I have two EC2 connectors with different regions for the same AWS account. How do I change them to cross-account role-based authentication?
You need to retain only one of the two connectors. Before you remove one of the connectors, ensure that you add the settings (for example, regions, tags, and activation) to the connector you plan to retain and then switch to cross-account role-based authentication.

How are my ARN details stored? Who has access to it?
ARN details are encrypted and stored in the database. The ARN configured is defined with READ-ONLY scope. This limits any other access and also controlled by users within their AWS account.

I am NOT seeing this support under my account?

This support is being rolled out currently to all the SaaS platforms and progressively to the Private platforms. Your POD is on the rollout schedule,you will see it soon.

For any issues or queries, please contact Qualys Support (support@qualys.com (mailto:support@qualys.com))