Monitoring AWS VPCs with Flow Logs

Stealthwatch Cloud

Introduction

VPC Flow Logs capture and record data about the IP traffic going to, coming from, and moving across your VPC. These records are used to drive the Stealthwatch Cloud service.

This document describes how to set up Flow Logs for your VPC and how to enable access the records.

Before starting, you'll need:

- An Amazon AWS account
- A web portal for Stealthwatch Cloud (formerly Observable Networks)

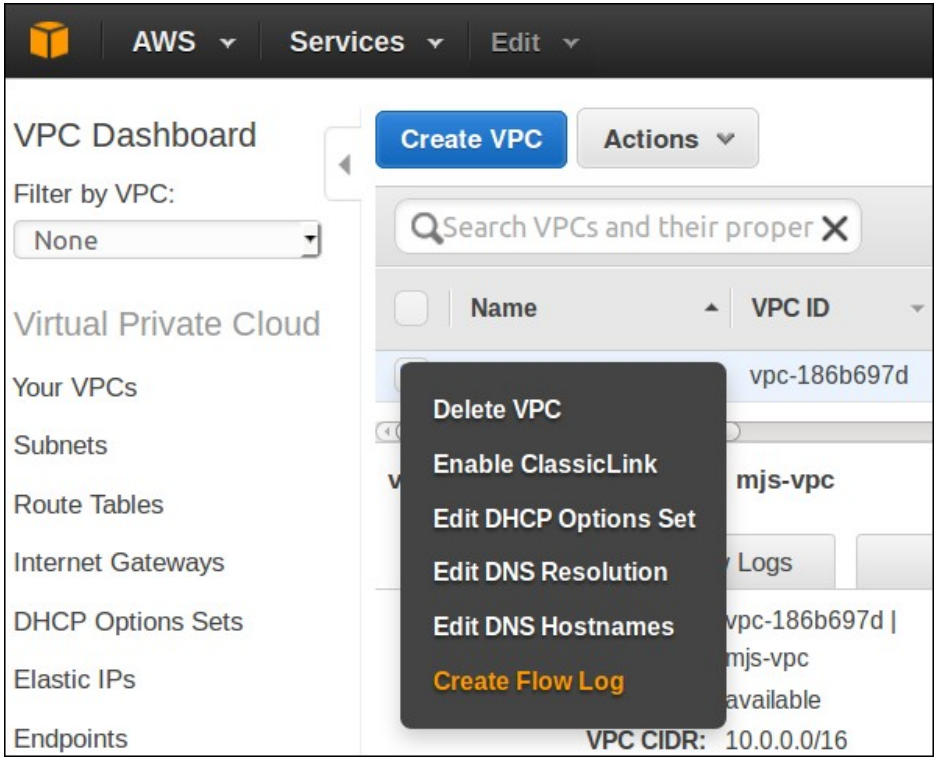
If you have questions or problems, please e-mail:
support@observable.net

Choose a VPC for monitoring

To start, go to the AWS Console for VPC management: https://console.aws.amazon.com/vpc/

Click on **Your VPCs** in the left pane.

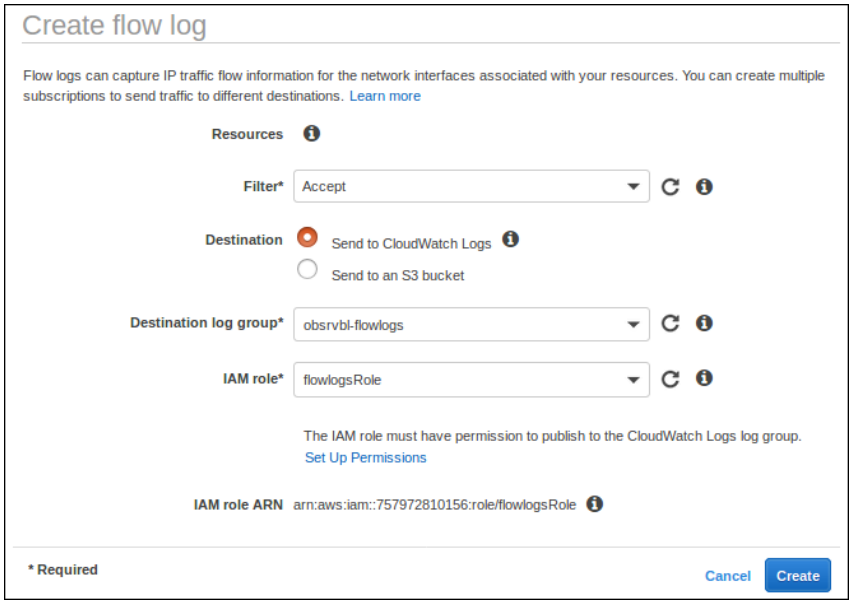
Right-click on a VPC and select **Create Flow Log** in the top-center pane.



Enable flow logging

Next, fill out the *Create flow log* form:

- **Filter:** Accept
- **Destination**: Send to CloudWatch Logs
- **Destination log group**: obsrvbl-flowlogs
- **IAM role**: flowlogsRole



If the *flowlogsRole* isn't available, click the **Set Up Permissions** link to create it.

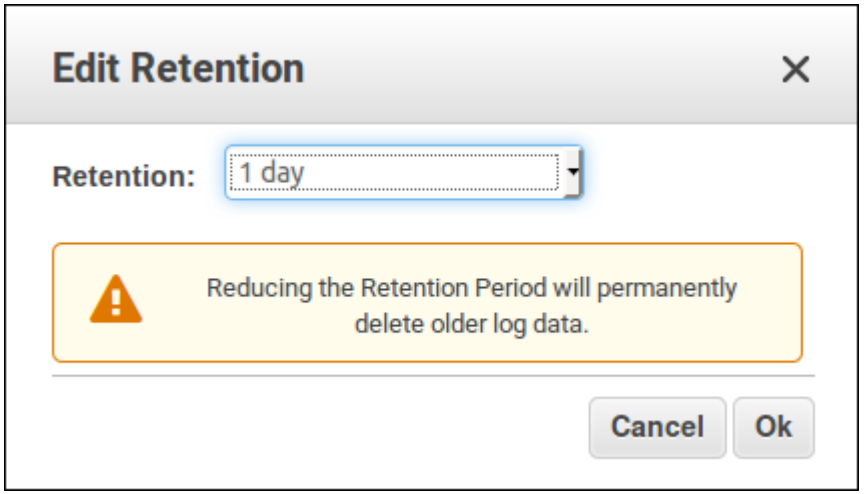
Note: Don't use the *obsrvbl_role* referenced later in this guide on this form; an internal AWS role is required here.

Set flow log retention

AWS charges for log storage, so be sure to set the retention period.

Go to the AWS Console for CloudWatch:
https://console.aws.amazon.com/cloudwatch

Select **Logs** on the left and then your new *obsrvbl-flowlogs* group. Click on the **Expire Events After** item to set the retention period to **1 day**.



IAM Policy

After your log group is created, you'll need to grant read access to it.

Go to the AWS Console for IAM: https://console.aws.amazon.com/iam

Click on **Policies** in the left pane.

Click on the **Create policy** button in the top-center pane.

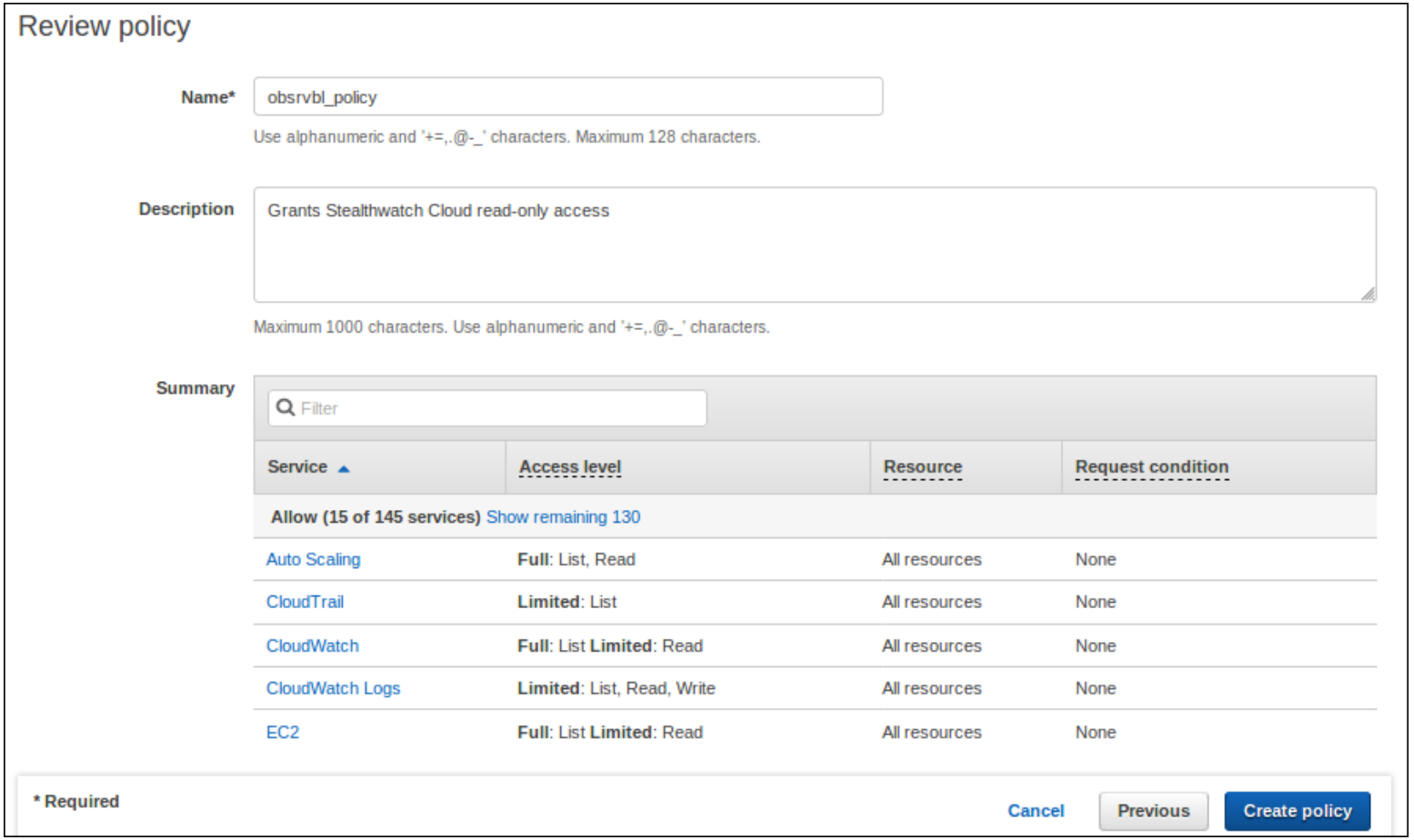
Click on the **JSON** tab.

Copy and paste the policy document from this page:
https://raw.githubusercontent.com/obsrvbl/aws-setup/master/obsrvbl-policy.json

Click **Review policy** to continue.

Review policy

After you've entered the policy, name it **obsrvbl_policy** and give it a description. Then click **Create policy**.



IAM Role

After the policy is created, you'll need to create an IAM Role that uses it.

Go to the AWS Console for IAM: https://console.aws.amazon.com/iam

Click on **Roles** in the left pane.

Click on the **Create Role** button in the top-center pane.

Select **Another AWS account** for the type of trusted entity.

Enter the following **Account ID**: 757972810156

Select **Require external ID** and then enter the domain of your web portal. This is the part of your web portal's address that comes before *.obsrvbl.com*.

- If your web portal is *example.obsrvbl.com*, then the external ID is *example*

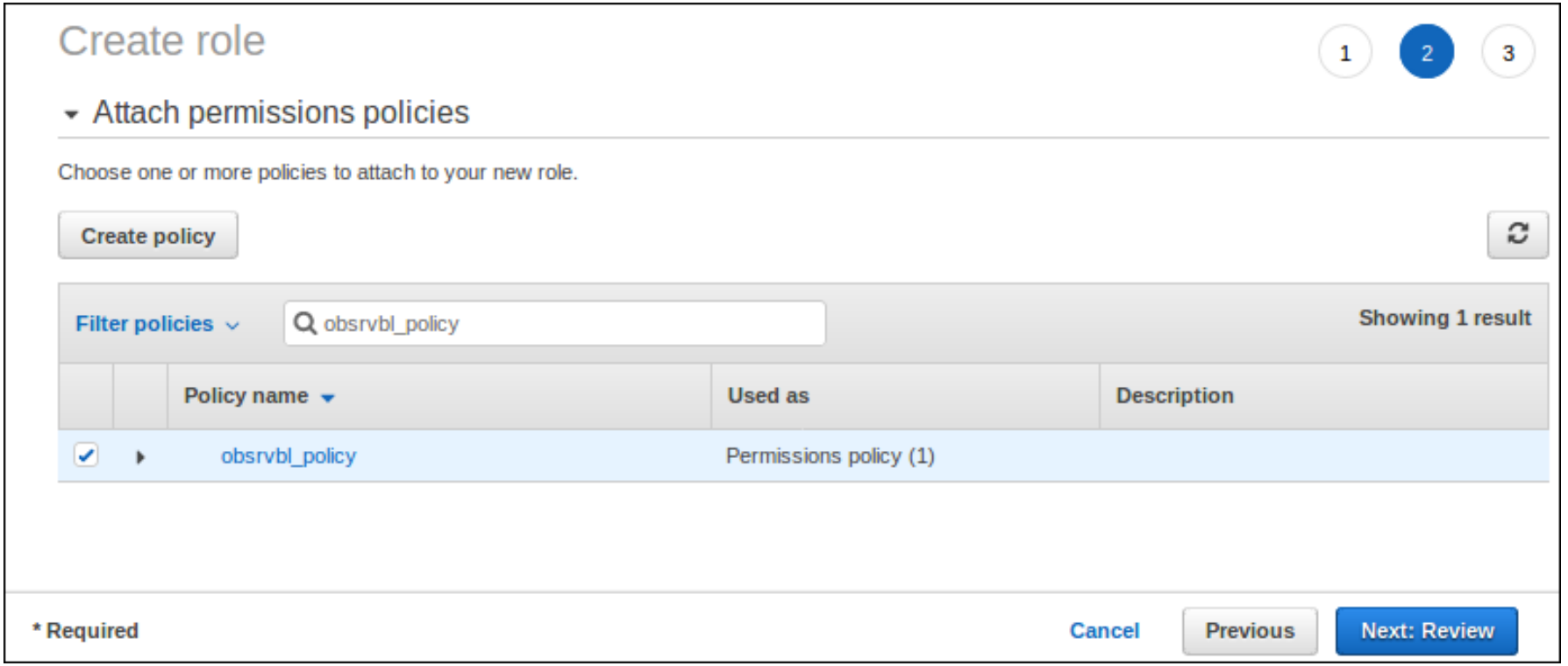
- If your web portal is *company.obsrvbl.com*, then the external ID is *company*

Finally, click **Next: Permissions**.

Role permissions

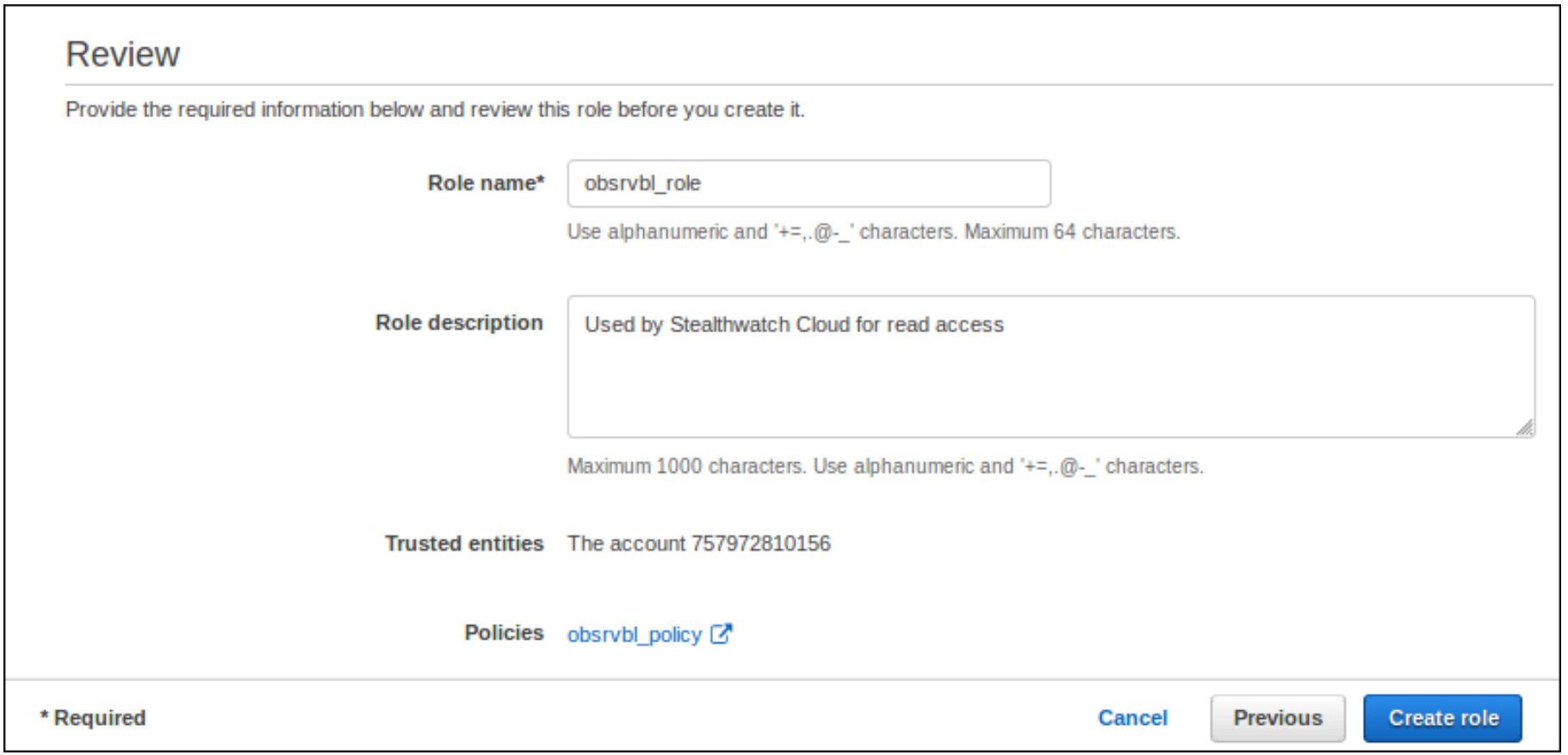
Under **Attach permissions policies**, search for the **obsrvbl_policy** you just created.

Click the check mark to select it and then on **Next: Review**.



Create a new Role

After you've attached the policy, name the role **obsrvbl_role** and add an optional description. Then click **Create role**.



Web portal configuration

Log in to your Stealthwatch Cloud web portal to configure it to query your AWS resources:

Click on the **Settings** icon (top-right corner).

Select the **Integrations** tab.

Select the **AWS** item.

Select the **Credentials** tab and enter the Role ARN from above.

Select the **VPC Flow** Logs tab and enter the CloudWatch group name you set up above.

If there is a problem with the credentials or log groups you will get an error message after entering them.

Troubleshooting

If you get an error message when adding the IAM role, double check the “External ID” you entered. It should match the subdomain for your web portal.

For example, for a web portal at https://customer.obsrvbl.com enter **customer** .

Finishing up

If everything is set up properly, you'll be able to see sensor data on the Stealthwatch Cloud web portal (on the Settings page under the *Sensors* tab).

To set up logs for additional VPCs, return to the AWS Console for VPC and create a new log. You won't have to set up the policies and roles again. Add the new group to the SWC web portal.

Again, if you have questions or problems with any of these steps: please e-mail support@observable.net.