**Following Security Group Best Practices**

### Introduction

In this Lab Step, you will begin investigating Trusted Advisor security recommendations starting with security groups. Security groups act as a firewall for EC2 instances deciding what traffic gets in and out. The consequences of letting too much traffic in are obvious, but at the same time, it can be tedious to track all security groups in all regions on your own. Trusted Advisor has a check to flag potentially vulnerable security group rules making the process much easier.

The check looks for unrestricted access to ports on inbound traffic. Any unrestricted port is given a status according to the following rules:

* No action is recommended for web traffic ports 80 (HTTP) and 443 (HTTPS), and mail ports 25 (SMTP) and 465 (SMTPS). That is due to the nature of the web and email which are expected to be accessed from anywhere.
* Action is recommended for certain file transfer and database ports. It is highly possible these services contain sensitive information and should be secured.
* Investigation is recommended for all other ports.

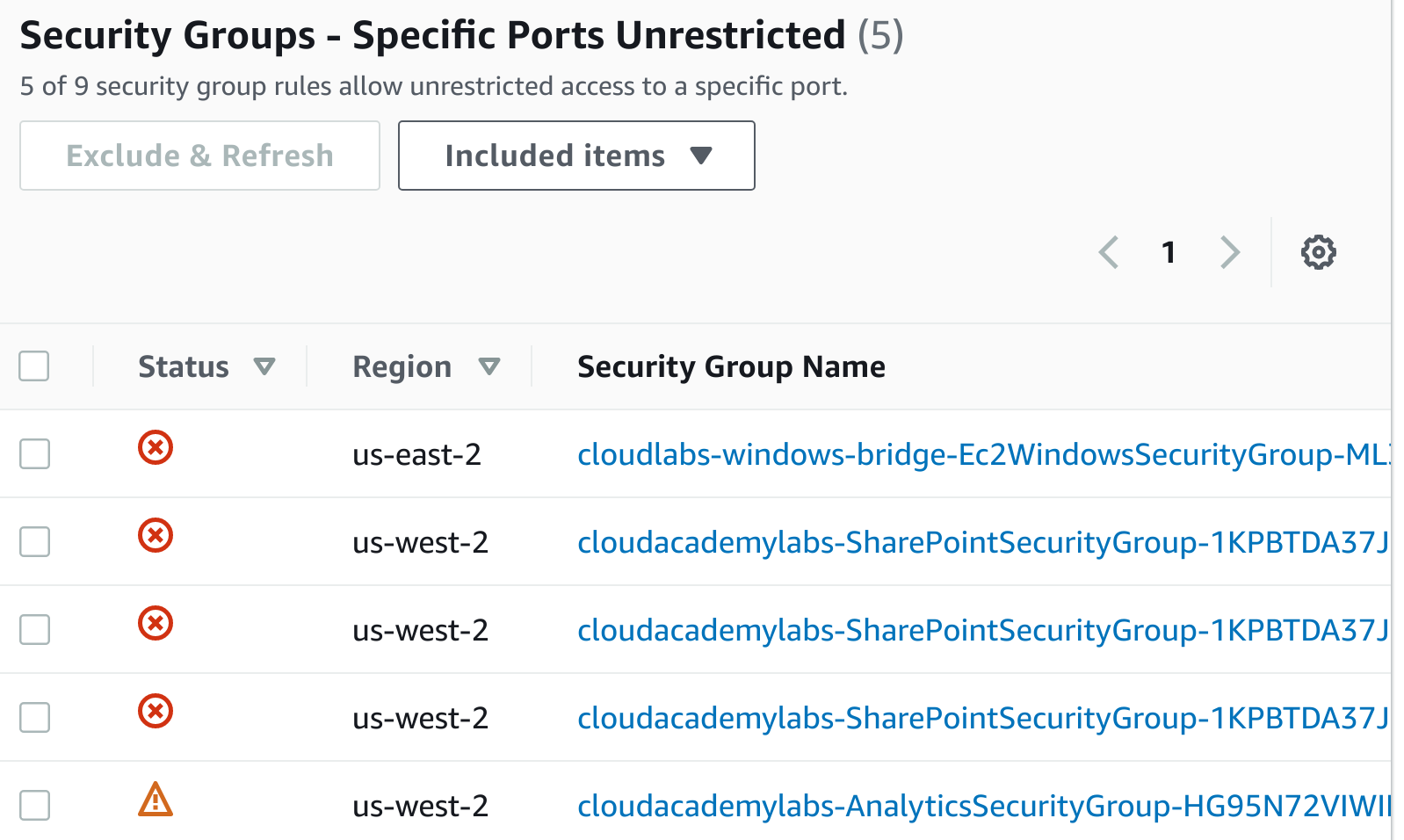
### Instructions

1. Navigate to **Dashboard > Security** within Trusted Advisor.

2. Click the triangle to the left of the **Security Groups - Specific Ports Unrestricted** check to expand the details.

The text describes the check criteria, provides useful **Additional Resources**, and a **Recommended Action**. You will take action on several security group rules to improve the AWS environment created for you by the Cloud Academy Lab environment.

3. Scroll down to focus on the table in the check details:



Note: You may have to scroll across the table to see all the columns.

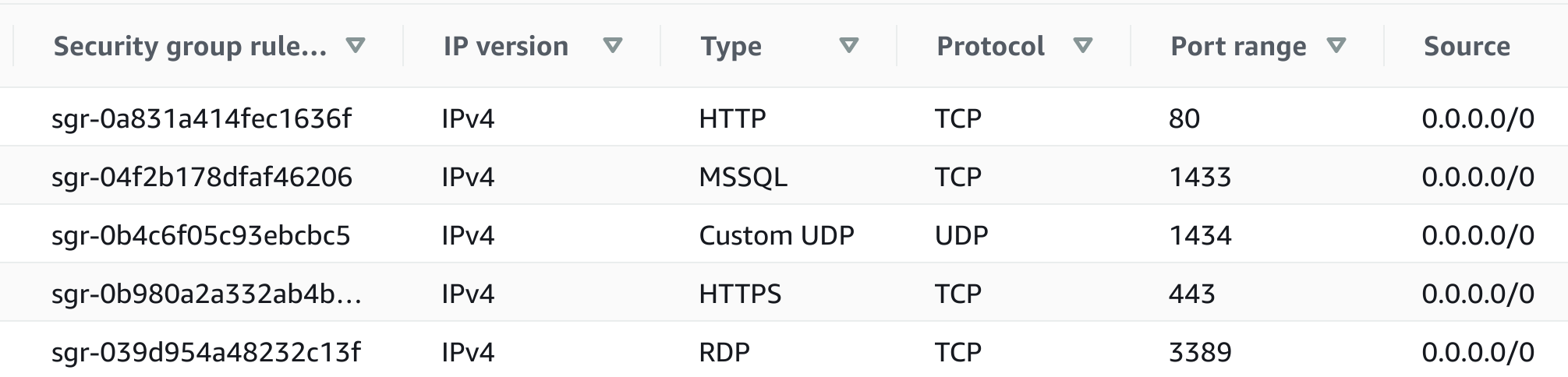
Four security group rules have been flagged. A security group used for hosting a Microsoft SharePoint service has three rules for which Trusted Advisor recommends action. You can identify the security group by locating **SharePoint** under the **Security Group Name** column. The ports are:

* tcp/1433 and udp/1434 used for SharePoint's Microsoft SQL Server database
* tcp/3389 use for Remote Desktop (RDP)

Note: You may see a security group with a name beginning with **cloudlabs-windows-bridge-Ec2WindowsSecurityGroup**. This security group is used to facilitate the lab's bridge functionality and should be ignored for the purposes of this lab.

4. Click on any of the **SharePoint**security group names to open up the security group details in the EC2 Console.

5. Click on the **Inbound rules** tab to see the inbound security group rules:



Notice that the SharePoint service also opened ports 80 and 443 with unrestricted access but Trusted Advisor knew not to raise a flag for those. You will resolve the **RDP** rule first by revoking the rule. Remote Desktop access is not required for the service and could have been an artifact of earlier development activity. The Microsoft SQL Server (**MS SQL**) port 1433 will be resolved by restricting access.

6. Click **Edit inbound rules** to begin editing the rules.

7. Click on **Delete** on the rightmost side of the **RDP**and **UDP 1434**rule to remove it.

8. Change the **Source** for the **MS SQL**rule from **0.0.0.0/0** to 54.42.123.0/24.

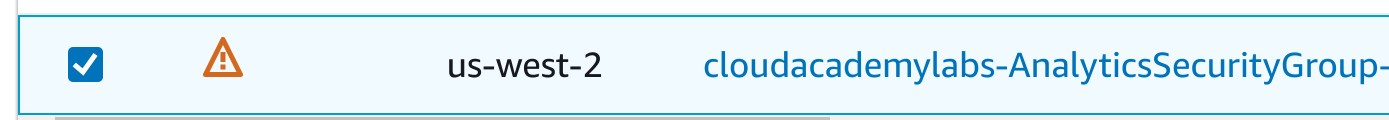
Making this change restricts the incoming traffic to IPs matching the specified Class C CIDR block. The specific block used in the instruction is arbitrary. In a production environment, only application servers in the block of IP addresses would continue to have access to the database.

9. Click **Save rules**.

10. Return to the security group table in Trusted Advisor.

The remaining flagged rule is for an Analytics dashboard service that implements it's own authorization and security measures. You know that the service is accessed remotely by various team members so restricting an IP range would be difficult. Having investigated the check and accepting the risk for unrestricted access to the port, you will exclude the rule from the check.

11. Check off the rule:



Note: You can also check the **cloudlabs-windows-bridge** security group if you see it.

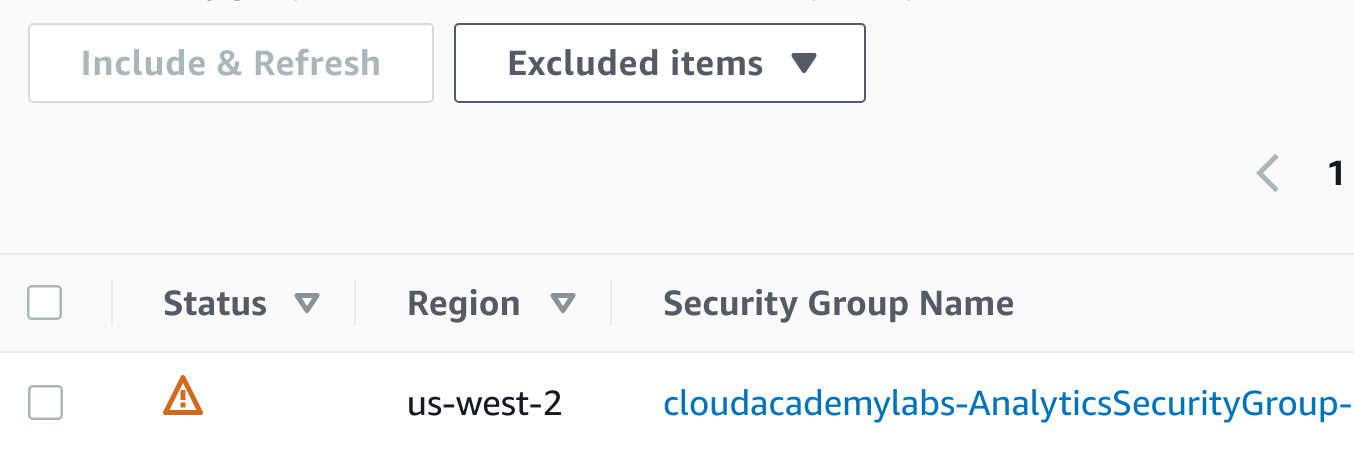
12. Click the **Exclude & Refresh** button just above the table.

Trusted Advisor will exclude the rule and begin processing the check. After a few seconds, you will see the results showing that no rules are flagged. The **Previous status: Red**is shown by the download button.

Warning: Due to delays internal to AWS, the **Exclude & Refresh** button may be greyed out for an unknown amount of time. However, the check and remainder of the lab is still functional. Please continue the lab and return to this step if you wish.

13. Select Excluded items from the **Item View** drop-down to the right of the **Exclude & Refresh** button.

You can always include any excluded rules by checking them off here and clicking **Include & Refresh**:



### Summary

In this Lab Step, you implemented best practices for security groups following Trusted Advisor's recommendations. You also saw how to exclude security group rules from Trusted Advisor's check.

VALIDATION CHECKS

**1Checks**

Check again

**The Security Group Has Been Fixed**

Check that the security group inbound rules have been fixed

Amazon EC2