Integrate ExtraHop with AWS CloudFormation

Published: 2018-07-16

This guide explains how to integrate the ExtraHop system with Amazon Web Services (AWS) CloudFormation. This guide assumes you have completed the procedure to install an EDA 1000v or EDA 2000v in AWS. You must have launched an ExtraHop AMI in the same region with the proper security groups configured to deploy a stack or monitor autoscaling groups.

Deploying a stack

To deploy a stack in CloudFormation, complete the following steps:

1. Go to `http://aws.amazon.com`
2. Click **My Account/Console**.
3. Select **AWS Management Console**.
4. Sign in with your username and password.
5. Go to `http://aws.amazon.com/cloudformation/aws-cloudformation-templates/`.
6. Right-click the template you want to use and save it to your workstation.
7. Open the template file in a text editor.
8. Define the ExtraHop IP and port by pasting the code at the end of the "`Parameters`" section as shown in the following example:

```
"EXTRAHOPIP" : {
    "DEFAULT" : "10.10.0.0",
    "DESCRIPTION" : "IP ADDRESS OF EXTRAHOP APPLIANCE",
    "TYPE" : "STRING"
},
"EXTRAHOPPORT" : {
    "DEFAULT" : "2003",
    "DESCRIPTION" : "PORT FOR EXTRAHOP FORWARDERS",
    "TYPE" : "STRING"
}
```

Note: Some PDF viewers might add extra newlines when copying and pasting commands. Ensure the text has copied correctly before running the command.

9. (Single stack) If you are deploying a single stack, format the user data script for CloudFormation by pasting the following code after `"#!/bin/bash", "\n",` in the "`User Data`" section:

```
"curl --connect-timeout 10 --fail -k 'https://", { "Ref" :
 "ExtraHopIP" }, "/tools/install-rpcapd.sh' > install-rpcapd.sh" ,"\n",
"sh install-rpcapd.sh ", { "Ref" : "ExtraHopIP" }, " ", { "Ref" :
 "ExtraHopPort" },"\n"
```

If the template you are using does not contain a "`User Data`" or `"#!/bin/bash", "\n",` section, you must create the sections to run this command formatted as follows:

```
"UserData" : {
    "Fn::Base64" : { "Fn::Join" : [ "", [
        "#!/bin/bash", "\n",
        "curl --connect-timeout 10 --fail -k 'https://", { "Ref" :
 "ExtraHopIP" }, "/tools/install-rpcapd.sh' > install-rpcapd.sh" ,"\n",
        "sh install-rpcapd.sh ", { "Ref" : "ExtraHopIP" }, " ", { "Ref" :
    "ExtraHopPort" },"\n"] ]
```

```
    }
}
```

Refer to the following example of the “Resources” attribute:

```
    "Resources" : {
        "Ec2Instance" : {
            "Type" : "AWS::EC2::Instance",
            "Properties" : {
            "SecurityGroups" : [ "security-group" ],
            "KeyName" : "key-name",
            "ImageId" : { "Ref" : "AMI" },
            "UserData" : {
            "Fn::Base64" : { "Fn::Join" : [ "", [
            "#!/bin/bash -v", "\n",
            "curl --connect-timeout 10 --fail -k 'https://", { "Ref" :
 "ExtraHopIP" }, "/tools/install-rpcapd.sh' > install-rpcapd.sh" ,"\n",
            "sh install-rpcapd.sh ", { "Ref" : "ExtraHopIP" }, " ",
 { "Ref" : "ExtraHopPort" },"\n"] ]
            }
        }
    }
}
}
```

(Autoscaling groups) If you are monitoring autoscaling groups, format the user data script for CloudFormation by pasting the following code after `"#!/bin/bash", "\n",` in the “`User Data`” section:

```
"curl --connect-timeout 10 --fail -k 'https://", { "Ref" :
 "ExtraHopIP" }, "/tools/install-rpcapd.sh' > install-rpcapd.sh" ,"\n",
"sh install-rpcapd.sh ", { "Ref" : "ExtraHopIP" }, " ", { "Ref" :
 "ExtraHopPort" },"\n"
```

Note: If the template you are using does not contain a “`User Data`” or `"#!/bin/bash", "\n",` section, you must create the sections to run this command formatted as follows:

```
"UserData" : {
    "Fn::Base64" : { "Fn::Join" : [ "", [
        "#!/bin/bash", "\n", "curl --connect-timeout 10 --fail
 -k 'https://", { "Ref" : "ExtraHopIP" }, "/tools/install-
rpcapd.sh' > install-rpcapd.sh" ,"\n",
        "sh install-rpcapd.sh ", { "Ref" : "ExtraHopIP" }, "
 ", { "Ref" : "ExtraHopPort" },"\n"] ]
    }
}
```

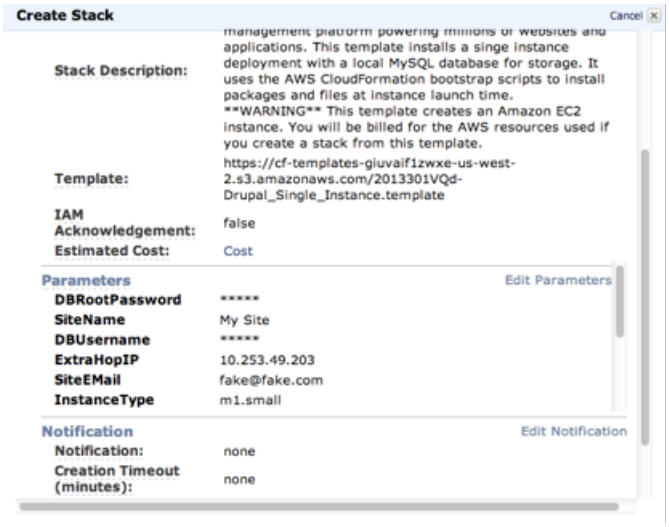
Refer to the following example of the “LaunchConfig” attribute:

```
"LaunchConfig": {
"Type" : "AWS::AutoScaling::LaunchConfiguration",
"Metadata" : {
...
},
"Properties": {
... "UserData" : { "Fn::Base64" : { "Fn::Join" : ["", [
"#!/bin/bash -v\n",
"curl --connect-timeout 10 -k 'https://[ExtraHopIP]/tools/install-
rpcapd.sh' > install-rpcapd.sh","\n",
"sh install-rpcapd.sh [ExtraHopIP] [Port]”]]
}
}
```

```
}
}
```

Note: Updating user data parameters will not change the packet forwarder settings on instances that have already been created. The user data field is processed only on instance initialization.

10. Save the template file.
11. Go to the CloudFormation Management Console at `https://console.aws.amazon.com/cloudformation`.
12. Click **Create New Stack**.
13. On the Create Stack page, complete the following actions:
    - **Stack Name:** Enter a name.
    - **Upload a Template File:** Select this radio button.
    - **Choose File:** Click this button and select the template file that you saved earlier.
14. Click **Continue**.
15. On the Specify Parameters page, enter the following parameters defined in the template:
    - **ExtraHopIP:** Enter your ExtraHop IP address.
    - **ExtraHopPort:** Enter the port number, which is 2003 by default.
16. Click **Continue**.
17. (Optional) From the Add Tags page, complete the Key and Value fields and click **Continue**.
18. Review the stack information (example below) and click **Continue**.



19. Click **Close**.
    After the browser redirects to the CloudFormation Management Console, view the status, which should be CREATE_IN_PROGRESS. When the stack has been built, the status changes to CREATE_COMPLETE.
20. Go to the EC2 management console.
21. Click the stack you just created and find the private IP.
22. Log in to the ExtraHop Web UI to analyze packet-forwarding traffic.

Analyze packet forwarding traffic in the ExtraHop Web UI

To find out how much forwarded traffic the ExtraHop system is receiving, complete the following steps.

1. Log in to the ExtraHop Web UI (`https://<extrahop_management_ip>/extrahop`) and click the **System Settings** icon in the top right corner.
2. Click **System Health** to get more information about the packet forwarding traffic.

   The RPCAP Packets and Throughput graphs contain four metrics:

   Encapsulation

   The total number of RPCAP encapsulation packets received by the ExtraHop system.

   Tunnel Eligible

   Total number of packets eligible to be forwarded to the ExtraHop system.

   Tunnel Sent

   Total number of RPCAP-tunneled packets forwarded to the ExtraHop system.

   Tunnel Received

   Total number of RPCAP-tunneled packets received by the ExtraHop system. The Tunnel Eligible, Tunnel Sent, and Tunnel Received values are equal if the ExtraHop system is receiving and processing all the packets sent by the server.

   If the Tunnel Eligible, Tunnel Sent, and Tunnel Received values do not equal the Tunnel Received values, refer to the following troubleshooting scenarios:

   - If Tunnel Sent is less than Tunnel Eligible, the server is not able to forward out all the traffic. This might indicate that packet forwarding requires more processing or outbound bandwidth resources on the instance. Consider separating the forwarding process onto a separate CPU or allocating a dedicated interface for forwarding traffic.
   - If Tunnel Received is less than Tunnel Sent, the ExtraHop system is not receiving all the traffic forwarded by the instance. This might be due to network congestion or insufficient resources on the ExtraHop system. If you suspect it is the latter, contact ExtraHop Support.