Integrieren Sie ExtraHop mit AWS CloudFormation

Veröffentlicht: 2023-09-30

In diesem Handbuch wird erklärt, wie RPCAP-Daemons auf EC2-Instances von ExtraHop installiert und konfiguriert werden. Sensoren wenn sie über Amazon Web Services (AWS) CloudFormation bereitgestellt werden.

In diesem Handbuch wird davon ausgegangen, dass Sie die folgenden Verfahren abgeschlossen haben einen ExtraHop-Sensor in AWS bereitstellen. Sie müssen in derselben Region ein ExtraHop-AMI mit den richtigen Sicherheitsgruppen gestartet haben, die für die Bereitstellung eines Stacks oder die Überwachung von Auto Scaling-Gruppen konfiguriert sind.

Einen Stack bereitstellen

Führen Sie die folgenden Schritte aus, um einen Stack in CloudFormation bereitzustellen.

1. Melden Sie sich bei Ihrer AWS-Managementkonsole an.
2. Laden Sie eine Beispielvorlage von der herunter AWS CloudFormation-Vorlagen Seite zu Ihrer Workstation. Wenn Sie bereits über eine Vorlage aus einer früheren Bereitstellung verfügen, bearbeiten Sie diese Vorlage mit den folgenden Änderungen.
3. Öffnen Sie die Vorlagendatei in einem Texteditor.
4. Definieren Sie die IP-Adresse und den Port des ExtraHop-Systems, indem Sie den Code am Ende des `"Parameters"` Abschnitt wie im folgenden Beispiel gezeigt:

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

Hinweis: Einige PDF-Viewer fügen beim Kopieren und Einfügen von Befehlen möglicherweise zusätzliche Zeilenumbrüche hinzu. Stellen Sie sicher, dass der Text korrekt ist, bevor Sie den Befehl ausführen.

5. (Einzelstapel) Wenn Sie einen einzelnen Stack bereitstellen, formatieren Sie das Benutzerdatenskript für CloudFormation, indem Sie den folgenden Code danach einfügen `"#!/bin/bash", "\n",` in der `"User Data"` Abschnitt:

```
"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"
```

Wenn Ihre Vorlage kein enthält `"User Data"` oder `"#!/bin/bash", "\n",` Abschnitt, Sie müssen die Abschnitte erstellen, um den Befehl auszuführen, formatiert wie im folgenden Beispiel:

```
"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"] ]
    }
}
```

Sehen Sie sich das folgende Beispiel für das Attribut „Resources“ an:

```
    "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"] ]
            }
        }
    }
}
}
```

(Auto Scaling-Gruppen) Wenn Sie Auto Scaling-Gruppen überwachen, formatieren Sie das Benutzerdatenskript für CloudFormation, indem Sie den folgenden Code danach einfügen `"#!/bin/bash", "\n",` in der `"User Data"` Abschnitt:

```
"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"
```

Wenn Ihre Vorlage kein enthält `"User Data"` oder `"#!/bin/bash", "\n",` Abschnitt, Sie müssen die Abschnitte erstellen, um diesen Befehl auszuführen, formatiert wie im folgenden Beispiel:

```
"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"] ]
    }
}
```

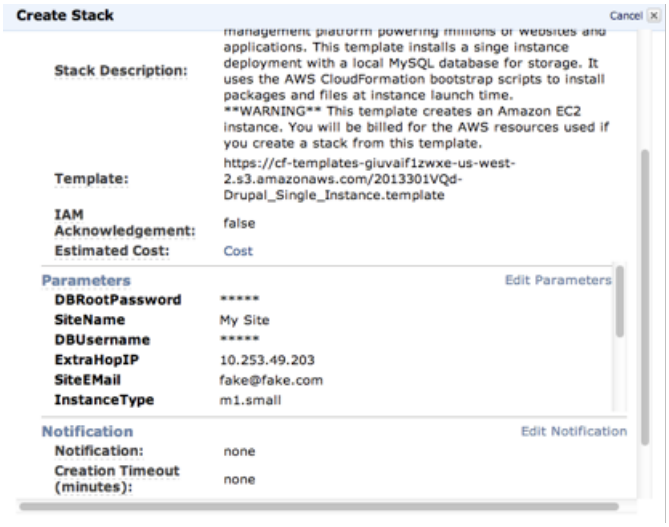
Sehen Sie sich das folgende Beispiel für das Attribut „launchConfig“ an:

```
"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]"]]
}
}
}
}
```

Hinweis: Durch das Aktualisieren von Benutzerdatenparametern werden die Paketweiterleitungseinstellungen für bereits erstellte Instanzen nicht geändert. Das Benutzerdatenfeld wird nur bei der Initialisierung der Instanz verarbeitet.

6. Speichern Sie die Vorlagendatei.
7. Klicken Sie auf den folgenden Link, um auf die CloudFormation Management Console zuzugreifen: `https://console.aws.amazon.com/cloudformation`.
8. klicken **Neuen Stack erstellen**.
9. Auf dem Stapel erstellen Seite, führe die folgenden Aktionen aus:
   - **Name des Stapels:** Geben Sie einen Namen ein.
   - **Laden Sie eine Vorlagendatei hoch:** Wählen Sie dieses Optionsfeld aus.
   - **Datei wählen:** Wählen Sie die Vorlagendatei aus, die Sie zuvor gespeichert haben.
10. klicken **Weiter**.
11. Auf dem Parameter angeben Seite, geben Sie die folgenden in der Vorlage definierten Parameter ein:
    - **Extra-Hop-IP:** Geben Sie die IP-Adresse Ihres ExtraHop-Systems ein.
    - **Zusätzlicher Hopport:** Geben Sie die Portnummer ein, die standardmäßig 2003 ist.
12. klicken **Weiter**.
13. Aus dem Schlagworte hinzufügen Seite, vervollständige die Schlüssel und Wert Felder, und klicken Sie dann auf **Weiter**.
14. Überprüfen Sie die Stack-Informationen und klicken Sie auf **Weiter**.
    Die folgende Abbildung zeigt konfigurierte Stack-Informationen.



15. klicken **Schliessen**.
    Nachdem der Browser zur CloudFormation Management Console umgeleitet wurde, sehen Sie sich den Status an. Dieser sollte `CREATE_IN_PROGRESS`. Wenn der Stack erstellt ist, ändert sich der Status zu `CREATE_COMPLETE`.
16. Navigieren Sie zur EC2-Managementkonsole.
17. Klicken Sie auf den Stack, den Sie gerade erstellt haben, und suchen Sie die private IP-Adresse.

18. Melden Sie sich beim ExtraHop-System an, um den Paketweiterleitungsverkehr zu analysieren.

Analysieren Sie den Paketweiterleitungsverkehr in der ExtraHop Web UI

Gehen Sie wie folgt vor, um herauszufinden, wie viel weitergeleiteten Verkehr das ExtraHop-System empfängt.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf **Systemeinstellungen** Symbol und dann klicken **Gesundheit des Systems** um mehr Informationen über den Paketweiterleitungsverkehr zu erhalten.

   Die RPCAP Pakete und Durchsatzdiagramme enthalten vier Metriken:

   Verkapselung
   Die Gesamtzahl der vom ExtraHop-System empfangenen RPCAP-Kapselungspakete.

   Geeignet für Tunnel
   Gesamtzahl der Pakete, die an das ExtraHop-System weitergeleitet werden können.

   Tunnel gesendet
   Gesamtzahl der RPCAP-Tunnelpakete, die an das ExtraHop-System weitergeleitet wurden.

   Tunnel empfangen
   Gesamtzahl der RPCAP-Tunnelpakete, die vom ExtraHop-System empfangen wurden. Die Werte „Tunnel Eligible“, „Tunnel Sent“ und „Tunnel Received“ sind identisch, wenn das ExtraHop-System alle vom Server gesendeten Pakete empfängt und verarbeitet.

   Wenn die Werte „Tunnel geeignet“, „Tunnel gesendet“ und „Tunnel empfangen“ nicht den Werten „Tunnel Received“ entsprechen, finden Sie in den folgenden Problembehandlungsszenarien weitere Informationen:

   - Wenn der Wert „Gesendeter Tunnel“ geringer als „Tunnel Eligible“ ist, kann der Server nicht den gesamten Datenverkehr weiterleiten. Dieser Zustand kann darauf hindeuten, dass die Paketweiterleitung mehr Verarbeitungs- oder ausgehende Bandbreitenressourcen auf der Instanz erfordert. Erwägen Sie, den Weiterleitungsprozess auf eine separate CPU aufzuteilen oder eine dedizierte Schnittstelle für die Weiterleitung des Datenverkehrs zuzuweisen.
   - Wenn Tunnel Received kleiner als Tunnel Sent ist, empfängt das ExtraHop-System nicht den gesamten von der Instance weitergeleiteten Traffic. Dieser Zustand kann auf eine Netzwerküberlastung oder unzureichende Ressourcen auf dem ExtraHop-System zurückzuführen sein. Wenn Sie vermuten, dass es sich um Letzteres handelt, wenden Sie sich an ExtraHop-Unterstützung.