Intégrer ExtraHop à AWS CloudFormation

Publié: 2023-09-19

Ce guide explique comment installer et configurer les démons rpcap sur les instances EC2 des capteurs ExtraHop lorsqu'ils sont déployés via Amazon Web Services (AWS) CloudFormation.

Ce guide suppose que vous avez effectué les procédures de déploiement d'un capteur ExtraHop dans AWS. Vous devez avoir lancé une AMI ExtraHop dans la même région avec les groupes de sécurité appropriés configurés pour déployer une pile ou surveiller les groupes de mise à l'échelle automatique.

Déployer une pile

Pour déployer une pile dans CloudFormation, procédez comme suit.

1. Connectez-vous à votre console de gestion AWS.
2. Téléchargez un modèle d'exemple à partir de la page Modèles AWS CloudFormation sur votre poste de travail. Si vous disposez déjà d'un modèle provenant d'un déploiement précédent, modifiez ce modèle avec les changements ci-dessous.
3. Ouvrez le fichier de modèle dans un éditeur de texte.
4. Définissez l'adresse IP et le port du système ExtraHop en collant le code à la fin de la section `"Parameters"`, comme indiqué dans l'exemple suivant :

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

   Note: Certaines visionneuses de PDF peuvent ajouter des lignes supplémentaires lors du copier-coller de commandes. Assurez-vous que le texte est correct avant d'exécuter la commande.

5. (Pile unique) Si vous déployez une pile unique, formatez le script de données utilisateur pour CloudFormation en collant le code suivant après `"#!/bin/bash", "\n",` dans la section `"User Data"`:

```
"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-"
```

   Si votre modèle ne contient pas de section `"User Data"` ou `"#!/bin/bash"`, `"\n"`, vous devez créer les sections nécessaires à l'exécution de la commande, formatées comme dans l'exemple suivant :

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

   Voir l'exemple suivant de l'attribut "Resources" :

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

(Groupes de mise à l'échelle automatique) Si vous surveillez des groupes de mise à l'échelle automatique, formatez le script de données utilisateur pour CloudFormation en collant le code suivant après `"#!/bin/bash", "\n",` dans la section `"User Data"`:

```
"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-"
```

Si votre modèle ne contient pas de section `"User Data"` ou `"#!/bin/bash", "\n",`, vous devez créer les sections nécessaires à l'exécution de cette commande, formatées comme dans l'exemple suivant :

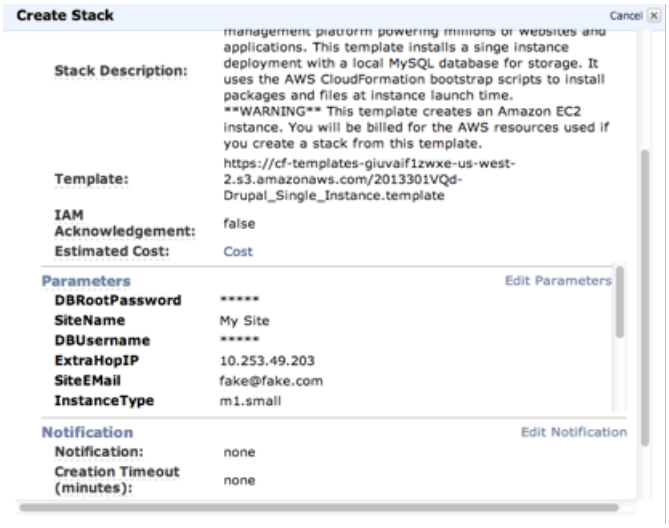
```
"UserData" : { "Fn::Base64" : { "Fn::Join" : [ "", [ "# !/bin/bash",
 "\N-", "curl --connect-timeout 10 --fail -k 'https://", { "Ref" :
 "ExtraHopIP" }, "/tools/install-rpcapd.sh' > install-rpcapd.sh" ,"\N-",
 "sh install-rpcapd.sh ", { "Ref" : "ExtraHopIP" }, " ", { "Ref" :
 "ExtraHopPort" },"\N-"]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

Voir l'exemple suivant de l'attribut "LaunchConfig" :

```
"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: La mise à jour des paramètres de données utilisateur ne modifiera pas les paramètres du transitaire de paquets sur les instances qui ont déjà été créées. Le champ des données utilisateur n'est traité que lors de l'initialisation de l'instance.

6. Enregistrez le fichier modèle.
7. Cliquez sur le lien suivant pour accéder à la console de gestion CloudFormation : `https://console.aws.amazon.com/cloudformation`.
8. Cliquez sur **Créer une nouvelle pile**.
9. Sur la page Créer une pile, effectuez les actions suivantes :
   - **Nom de la pile:** Saisissez un nom.
   - **Télécharger un fichier modèle:** Sélectionnez cette case d'option.
   - **Choisir un fichier:** Sélectionnez le fichier modèle que vous avez enregistré précédemment.
10. Cliquez sur **Continuer**.
11. Sur la page Specify Parameters, entrez les paramètres suivants définis dans le modèle :
    - **ExtraHopIP:** Saisissez l'adresse IP de votre système ExtraHop.
    - **ExtraHopPort:** Saisissez le numéro de port, qui est 2003 par défaut.
12. Cliquez sur **Continuer**.
13. Dans la page Ajouter des balises, remplissez les champs Clé et Valeur, puis cliquez sur **Continuer**.
14. Passez en revue les informations relatives à la pile et cliquez sur **Continuer**.
    La figure suivante présente les informations de la pile configurée.



15. Cliquez sur **Fermer**.
    Une fois que le navigateur est redirigé vers la console de gestion CloudFormation, affichez l'état, qui devrait être `CREATE_IN_PROGRESS`. Lorsque la pile est construite, l'état devient `CREATE_COMPLETE`.
16. Accédez à la console de gestion EC2.
17. Cliquez sur la pile que vous venez de créer et recherchez l'adresse IP privée.
18. Connectez-vous au système ExtraHop pour analyser le trafic de transfert de paquets.

Analyse du trafic de transfert de paquets dans l'interface Web ExtraHop

Pour connaître la quantité de trafic transféré que reçoit le système ExtraHop, procédez comme suit.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône **Paramètres système** puis sur **Santé du système** pour obtenir plus d'informations sur le trafic de transfert de paquets.

   Les graphiques RPCAP Packets et Throughput contiennent quatre mesures :

   Encapsulation
   Nombre total de paquets d'encapsulation RPCAP reçus par le système ExtraHop.

   Tunnel éligible
   Nombre total de paquets pouvant être transmis au système ExtraHop.

   Tunnel envoyé
   Nombre total de paquets à tunnel RPCAP transmis au système ExtraHop.

   Tunnel reçu
   Nombre total de paquets à tunnel RPCAP reçus par le système ExtraHop. Les valeurs Tunnel Eligible, Tunnel Sent et Tunnel Received sont égales si le système ExtraHop reçoit et traite tous les paquets envoyés par le serveur.

   Si les valeurs du tunnel admissible, du tunnel envoyé et du tunnel reçu ne sont pas égales aux valeurs du tunnel reçu, reportez-vous aux scénarios de dépannage suivants :

   - Si le tunnel envoyé est inférieur au tunnel éligible, le serveur n'est pas en mesure de transmettre tout le trafic. Cette condition peut indiquer que le transfert de paquets nécessite plus de ressources de traitement ou de bande passante sortante sur l'instance. Envisagez de séparer le processus de transfert sur une unité centrale distincte ou d'allouer une interface dédiée au transfert du trafic.

- Si le tunnel reçu est inférieur au tunnel envoyé, le système ExtraHop ne reçoit pas tout le trafic transféré par l'instance. Cette situation peut être due à une congestion du réseau ou à des ressources insuffisantes sur le système ExtraHop. Si vous pensez que c'est le cas, contactez l'assistance ExtraHop.