

Intégrez ExtraHop à AWS CloudFormation

Publié: 2024-08-08

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

Ce guide part du principe que vous avez suivi les procédures pour [déployer une sonde 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 des groupes Auto Scaling.

Déploiement d'une pile

Pour déployer une pile dans CloudFormation, procédez comme suit.

1. Connectez-vous à votre console de gestion AWS.
2. Téléchargez un exemple de modèle à partir du [Modèles AWS CloudFormation](#) page vers votre poste de travail. Si vous possédez déjà un modèle issu d'un déploiement précédent, modifiez-le avec les modifications ci-dessous.
3. Ouvrez le fichier modèle dans un éditeur de texte.
4. Définissez l'adresse IP et le port du système ExtraHop en collant le code à la fin du "Parameters" section 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 de nouvelles lignes supplémentaires lors du copier-coller des commandes. Assurez-vous que le texte est correct avant d'exécuter la commande.

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

Si votre modèle ne contient pas de "User Data" ou "#!/bin/bash", "\n", section, vous devez créer les sections pour exécuter 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" ] ] }
}
```

}

Reportez-vous à 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 Auto Scaling) Si vous surveillez des groupes Auto Scaling, formatez le script de données utilisateur pour CloudFormation en collant le code suivant après "#!/bin/bash", "\n", dans le "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"

```

Si votre modèle ne contient pas de "User Data" ou "#!/bin/bash", "\n", section, vous devez créer les sections pour exécuter 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" ] ]
  }
}

```

Reportez-vous à 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]" ] ]
    }
  }
}

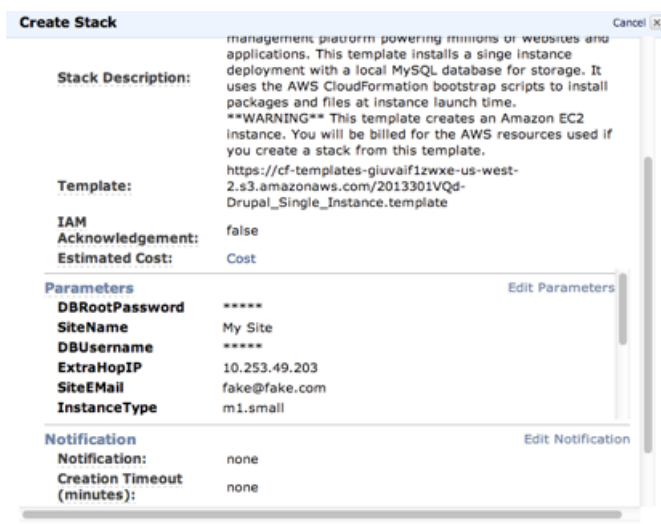
```



Note: La mise à jour des paramètres des données utilisateur ne modifiera pas les paramètres du redirecteur de paquets sur les instances déjà créées. Le champ de données utilisateur est traité uniquement 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 **Créer une nouvelle pile**.
9. Sur le Créer une pile page, effectuez les actions suivantes :
 - **Nom de la pile:** Entrez un nom.
 - **Charger un fichier modèle:** Sélectionnez ce bouton radio.
 - **Choisissez un fichier:** Sélectionnez le fichier modèle que vous avez enregistré précédemment.
10. Cliquez **Poursuivre**.
11. Sur le Spécifier les paramètres page, entrez les paramètres suivants définis dans le modèle :
 - **Hop IP supplémentaire:** Entrez l'adresse IP de votre système ExtraHop.
 - **Port Hoppport supplémentaire:** Entrez le numéro de port, qui est 2003 par défaut.
12. Cliquez **Poursuivre**.
13. À partir du Ajouter des tags page, complétez le Clé et Valeur champs, puis cliquez sur **Poursuivre**.
14. Passez en revue les informations de la pile et cliquez sur **Poursuivre**.

La figure suivante montre les informations de pile configurées.



15. Cliquez **Fermer**.
Une fois le navigateur redirigé vers la console de gestion CloudFormation, consultez l'état, qui devrait être `CREATE_IN_PROGRESS`. Lorsque la pile est créée, le statut passe à `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.

Analyser le trafic de transfert de paquets dans l'interface utilisateur Web ExtraHop

Pour connaître le volume 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 le **Réglages du système** icône  puis cliquez sur **État du système** pour obtenir plus d'informations sur le trafic de transfert de paquets.

Le RPCAP Les graphiques de paquets et de débit contiennent quatre métriques :

Encapsulation

Le nombre total de paquets d'encapsulation RPCAP reçus par le système ExtraHop.

Tunnel éligible

Nombre total de paquets éligibles à être transférés vers le système ExtraHop.


Tunnel envoyé

Nombre total de paquets tunnelisés RPCAP transmis au système ExtraHop.

Tunnel reçu

Nombre total de paquets tunnelisés RPCAP reçus par le système ExtraHop. Les valeurs Tunnel Éligible, Tunnel Sent et Tunnel Recived sont égales si le système ExtraHop reçoit et traite tous les paquets envoyés par le serveur.

Si les valeurs du tunnel éligible, 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 à la valeur éligible au tunnel, le serveur n'est pas en mesure de transférer tout le trafic. Cette condition peut indiquer que le transfert de paquets nécessite davantage de ressources de traitement ou de bande passante sortante sur l'instance. Envisagez de séparer le processus de transfert sur un processeur distinct 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 condition peut être due à un encombrement du réseau ou à des ressources insuffisantes sur le système ExtraHop. Si vous pensez qu'il s'agit de ce dernier cas, contactez [Assistance ExtraHop](#) .