

Déployez une sonde ExtraHop sur Google Cloud Platform

Publié: 2024-01-22


Les procédures suivantes expliquent comment déployer un ExtraHop virtuel. sonde dans un environnement Google Cloud. Vous devez avoir de l'expérience dans le déploiement de machines virtuelles dans Google Cloud au sein de votre infrastructure de réseau virtuel.


Pour garantir le succès du déploiement, assurez-vous d'avoir accès et de pouvoir créer les ressources requises. Vous devrez peut-être travailler avec d'autres experts de votre organisation pour vous assurer que les ressources nécessaires sont disponibles.

Exigences du système

Votre environnement doit répondre aux exigences suivantes pour déployer un ExtraHop virtuel sonde dans GCP :

- Vous devez disposer d'un compte Google Cloud Platform (GCP)
- Vous devez disposer du fichier de déploiement ExtraHop, qui est disponible sur [Portail client ExtraHop](#) 
- Vous devez disposer d'une clé de produit ExtraHop.
- La mise en miroir des paquets doit être activée dans GCP pour transférer le trafic réseau vers le système ExtraHop. La mise en miroir des paquets doit être configurée pour envoyer le trafic à nic1 (et non à nic0) de l'instance ExtraHop. Voir <https://cloud.google.com/vpc/docs/using-packet-mirroring> 

 **Important:** Pour garantir les meilleures performances lors de la synchronisation initiale de l'équipement, connectez tous les capteurs à la console, puis configurez le transfert du trafic réseau vers les capteurs.

- Vous devez configurer des règles de pare-feu pour autoriser le trafic DNS, HTTP, HTTPS et SSH pour l'administration d'ExtraHop. Voir <https://cloud.google.com/vpc/docs/using-firewalls> 
- Vous devez fournir un type d'instance GCP qui correspond le mieux à l'instance virtuelle sonde taille, comme suit :

capteur	Type d'instance recommandé
Reveal (x) EDA 1100 v	n1-standard-4 (4 vCPU, 15 Go de mémoire)

Téléchargez le fichier de déploiement ExtraHop

1. Connectez-vous à votre compte Google Cloud Platform.
2. Dans le menu de navigation, cliquez sur **Stockage dans le cloud** > **Navigateur**.
3. Cliquez sur le nom du bucket de stockage dans lequel vous souhaitez télécharger le fichier de déploiement ExtraHop. Si vous ne disposez pas d'un bucket de stockage préconfiguré, créez-en un dès maintenant.
4. Cliquez **Téléverser des fichiers**.
5. Naviguez jusqu'au `extrahop-eda-gcp-<version>.tar.gz` fichier que vous avez précédemment téléchargé et cliquez sur **Ouvert**. Attendez que le fichier soit chargé, puis passez à la procédure suivante.

Créez l'image

1. Dans le menu de navigation, cliquez sur **Moteur de calcul** > **Des images**.


2. Cliquez **Créer une image** et effectuez les étapes suivantes :
 - a) Dans le Nom champ, saisissez un nom pour identifier la sonde ExtraHop.
 - b) Dans la liste déroulante Source, sélectionnez **Fichier de stockage dans le cloud**.
 - c) Dans le Fichier de stockage dans le cloud section, cliquez **Parcourez**, localisez le `extrahop-eda-gcp-<version>.tar.gz` fichier dans votre compartiment de stockage, puis cliquez sur **Sélectionnez**.
 - d) Configurez tous les champs supplémentaires requis pour votre environnement.
3. Cliquez **Créez**.

Création du disque de la banque de données

1. Dans le menu de navigation, cliquez sur **Moteur de calcul > Disques**.
2. Cliquez **Créer un disque** et effectuez les étapes suivantes :
 - a) Dans le Nom dans ce champ, saisissez un nom pour identifier le disque ExtraHop.
 - b) À partir du Type menu déroulant, sélectionnez **Disque persistant standard**.
 - c) Dans le Type de source section, cliquez **Image**.
 - d) À partir du La source liste déroulante des images, sélectionnez l'image que vous avez créée lors de la procédure précédente.
 - e) Dans le Taille champ, type 61.
 - f) Configurez tous les champs supplémentaires requis pour votre environnement.
3. Cliquez **Créez**.


Création de l'instance de machine virtuelle


1. Dans le menu de navigation, cliquez sur **Moteur de calcul > Instances de machines virtuelles**.
2. Cliquez **Créer une instance** et effectuez les étapes suivantes :
 - a) Dans le Nom champ, saisissez un nom pour identifier l'instance ExtraHop.
 - b) Dans la liste déroulante Région, sélectionnez votre région géographique.
 - c) Dans la liste déroulante Zone, sélectionnez un emplacement au sein de votre zone géographique.
 - d) Dans le Configuration de la machine section, sélectionnez **Usage général** pour la famille de machines, **N1** pour la série, et **n1-standard-4 (4 vCPU, 15 Go de mémoire)** pour le type de machine.
 - e) Dans le Disque de démarrage section, cliquez **Changez**.
 - f) Cliquez **Disques existants**.
 - g) À partir du Disque liste déroulante, sélectionnez le disque que vous avez créé lors de la procédure précédente.
 - h) Cliquez **Sélectionnez**.
3. Cliquez **Options avancées**.
4. Cliquez **Réseautage**.
5. Dans le champ Balises réseau, saisissez les noms de balises suivants :

 **Important:** Les balises réseau sont nécessaires pour appliquer des règles de pare-feu à l'instance ExtraHop. Si aucune règle de pare-feu n'autorise ce trafic, vous devez créer ces règles. Voir <https://cloud.google.com/vpc/docs/using-firewalls>.

- serveur https
- serveur http
- dns
- ssh-all



6. Dans le Interfaces réseau section, cliquez sur l'icône d'édition  pour modifier l'interface de management.
 - a) À partir du **Réseau** liste déroulante, sélectionnez votre réseau de gestion.
 - b) À partir du **Sous-réseau** dans la liste déroulante, sélectionnez le sous-réseau de votre réseau de gestion.
 - c) Configurez tous les champs supplémentaires requis pour votre environnement.
 - d) Cliquez **Terminé**.
7. Cliquez **Ajouter une interface réseau** pour configurer l' interface de capture de données.

 **Important:** L'interface de gestion et l'interface de capture de données doivent se trouver dans des réseaux de cloud privé virtuel (VPC) différents.

 - a) À partir du **Réseau** liste déroulante, sélectionnez votre réseau qui reflétera le trafic vers le système ExtraHop.
 - b) À partir du **Sous-réseau** liste déroulante, sélectionnez votre sous-réseau.
 - c) À partir du **IP externe** liste déroulante, sélectionnez **Aucune**.
 - d) Configurez tous les champs supplémentaires requis pour votre environnement.
 - e) Cliquez **Terminé**.
8. Cliquez **Créez**.

Création d'un groupe d'instances

1. Dans le volet gauche du Moteur de calcul page, cliquez **Groupes d'instances**.
2. Cliquez **Créer un groupe d'instances**.
3. Cliquez **Nouveau groupe d'instances non géré**.
4. Entrez un nom de groupe d'instances dans le **Nom** champ.
5. Dans le Réseau et instances section, sélectionnez le réseau auquel l'instance peut accéder depuis **Réseau** liste déroulante.
6. Sélectionnez le sous-réseau dans le **Sous-réseau** liste déroulante.
7. Sélectionnez la sonde dans **Sélectionnez une machine virtuelle** liste déroulante.
8. Cliquez **Créez**.

Création d'un équilibreur de charge

1. Sur le Services de réseau page, cliquez **équilibrage de charge**.
2. Cliquez **Créer un équilibreur de charge**.
3. Dans le Équilibrage de charge UDP section, cliquez **Démarrer la configuration**.
4. Sélectionnez **Uniquement entre mes machines virtuelles**.
5. Cliquez **Poursuivre**.
6. Entrez le nom de l'équilibreur de charge.
7. Sélectionnez votre région dans **Région** liste déroulante.
8. Sélectionnez votre réseau dans **Réseau** liste déroulante.
9. Dans le Nouveau backend section, sélectionnez votre groupe d'instances dans la liste déroulante.
10. Cliquez **Bilan de santé** puis cliquez sur **Créer un bilan de santé**.

11. Entrez le nom du bilan de santé.
12. Sélectionnez **TCP** dans la liste déroulante Protocol.
13. Type 443 dans le champ Port.
14. Cliquez **Enregistrer**.

Création d'une politique de mise en miroir du trafic

1. Sur la page Réseau VPC, cliquez sur **Mise en miroir de paquets**.
2. Cliquez **Créer une politique**.
3. Dans le Définir la vue d'ensemble des politiques section, entrez un nouveau nom de politique.
4. Sélectionnez votre région dans **Région** liste déroulante.
5. Cliquez **Poursuivre**.
6. Sélectionnez **La source et la destination du collecteur mises en miroir se trouvent dans le même réseau VPC**.
7. Sélectionnez le réseau VPC dans **Réseau** liste déroulante.
8. Cliquez **Poursuivre**.
9. Sélectionnez le **Sélectionnez un ou plusieurs sous-réseaux** case à cocher.
10. À partir du **Sélectionnez un sous-réseau** liste déroulante, cochez la case à côté de votre sous-réseau.
11. Sélectionnez le **Sélectionnez des instances individuelles** case à cocher.
12. Cliquez **Sélectionnez**.
13. Cochez la case à côté de l'instance de machine virtuelle.
14. Cliquez **Poursuivre**.
15. Sélectionnez l'équilibreur de charge que vous avez créé précédemment dans **Destination du collectionneur** liste déroulante.
16. Cliquez **Poursuivre**.
17. Sélectionnez **Refléter tout le trafic (par défaut)**.
18. Cliquez **Soumettre**.

Configuration de la sonde

Après avoir configuré une adresse IP pour sonde, ouvrez un navigateur Web et accédez au système ExtraHop via l'adresse IP configurée. Acceptez le contrat de licence, puis connectez-vous. Le nom de connexion par défaut est `setup` et le mot de passe est `default`. Suivez les instructions pour saisir la clé de produit, modifier la configuration par défaut et les mots de passe du compte utilisateur shell, vous connecter aux services cloud ExtraHop et vous connecter à une console ExtraHop.

Une fois que le système a obtenu une licence et que vous avez vérifié que le trafic est détecté, suivez les procédures recommandées dans [liste de contrôle après le déploiement](#).

Configurer la découverte des équipements L3

Vous devez configurer le système ExtraHop pour découvrir et suivre les appareils locaux et distants par leur adresse IP (L3 Discovery). Pour savoir comment fonctionne la découverte d'équipements dans le système ExtraHop, voir [Découverte des appareils](#).

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez **Capture**.
3. Cliquez **Découverte des appareils**.

4. Dans le Découverte des appareils locaux section, sélectionnez **Activer la découverte des équipements locaux** case à cocher pour activer L3 Discovery .
5. Dans le Découverte d'appareils à distance section, saisissez l' adresse IP dans le Plages d'adresses IP champ. Vous pouvez spécifier une adresse IP ou une notation CIDR, telle que 192.168.0.0/24 pour un réseau IPv4 ou 2001:db8::/32 pour un réseau IPv6.
6. Cliquez **Enregistrer**.