Déployez une sonde ExtraHop sur Google Cloud Platform

Publié: 2024-04-10

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

Un ExtraHop virtuel sonde peut vous aider à surveiller les performances de vos applications sur les réseaux internes, l' Internet public ou une interface de bureau virtuel (VDI), y compris la base de données et les niveaux de stockage. Le système ExtraHop peut surveiller les performances des applications dans des environnements géographiquement distribués, tels que des succursales ou des environnements virtualisés via le trafic inter-machines virtuelles.

Cette installation vous permet d'exécuter la surveillance des performances du réseau, la détection et la réponse du réseau, ainsi que la détection des intrusions sur un seul sonde.

Note: Si vous avez activé le module IDS sur cette sonde et que votre système ExtraHop n'a pas d'accès direct à Internet ni aux services ExtraHop Cloud, vous devrez télécharger les règles IDS manuellement. Pour plus d'informations, voir Téléchargez les règles IDS dans le système ExtraHop via l'API REST.

Pour garantir la réussite 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, disponible sur le Portail client ExtraHop.
- Vous devez avoir un ExtraHop sonde clé de produit.
- 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 vers nic1 (et non vers 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.
- Les règles de pare-feu doivent être configurées pour autoriser le trafic DNS, HTTP, HTTPS et SSH pour l'administration d' ExtraHop. Voir https://cloud.google.com/vpc/docs/using-firewalls.

Exigences relatives aux machines virtuelles

Vous devez provisionner le type d'instance GCP qui correspond le mieux à la taille de votre sonde virtuelle ExtraHop et qui répond aux exigences de module suivantes.

Sonde	Modules	Type d'instance recommandé	Taille du disque de la banque de données
Reveal (x) EDA 1100v	EDA	n1-standard-4 (4 processeurs virtuels et 15 Go de mémoire)	61 GO
	EDA + IDS	n2-standard-32 (32 processeurs virtuels et 128 Go de mémoire)	1400 GO

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** > **Seaux**.
3. Cliquez sur le nom du compartiment de stockage dans lequel vous souhaitez télécharger le fichier de déploiement ExtraHop.

   Si vous n'avez pas de compartiment de stockage préconfiguré, créez-en un maintenant.
4. Cliquez **Charger des fichiers**.
5. Naviguez jusqu'au `extrahop-<module>-gcp-<version>.tar.gz` fichier que vous avez précédemment téléchargé et cliquez sur **Ouvrir**.

Prochaines étapes
Une fois le téléchargement du fichier terminé, vous pouvez créer l'image.

Créez l'image

1. Dans le menu de navigation, cliquez sur **Moteur de calcul** > **Images**.
2. Cliquez **Créer une image**.
3. Dans le Nom dans le champ, saisissez un nom pour identifier la sonde ExtraHop.
4. Dans la liste déroulante Source, sélectionnez **Fichier Cloud Storage**.
5. Dans le Fichier Cloud Storage section, cliquez sur **Parcourir**, localisez le `extrahop-eda-gcp-<version>.tar.gz` fichier dans votre compartiment de stockage, puis cliquez sur **Sélectionnez**.
6. Configurez tous les champs supplémentaires requis pour votre environnement.
7. Cliquez **Code équivalent**.

   Un panneau s'ouvre sur la droite.
8. Dans le panneau Code équivalent, cliquez sur **Copier**.
9. Cliquez **Exécuter dans Cloud Shell**.

   Le texte copié s'affiche lorsque vous y êtes invité.
10. Ajoutez cette option à la fin de la séquence de commandes :

    `--Guest-OS-Features=GVNIC`
11. Appuyez sur ENTER.

Prochaines étapes
Une fois la commande exécutée, fermez Cloud Shell, puis cliquez sur **Annuler**. En cliquant **Annuler** n' annule pas la création de l'image via Cloud Shell.

Création du disque de banque de données

1. Dans le volet de gauche, Moteur de calcul page, cliquez sur **Disques**.

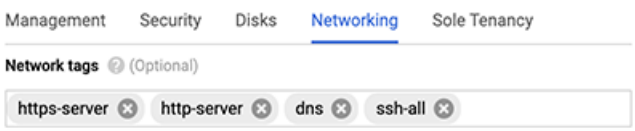
2. Cliquez **Créer un disque**.
3. Dans le Nom dans le champ, saisissez un nom pour identifier le disque ExtraHop.
4. À partir du Type de source de disque liste déroulante, cliquez sur **Image**.
5. À partir du Type de disque liste déroulante, sélectionnez **Disque persistant standard**.
6. À partir du Source dans la liste déroulante des images, sélectionnez l'image que vous avez créée précédemment.
7. Dans le Taille dans ce champ, saisissez une valeur, en Go, pour la taille du disque.

   Pour plus d'informations sur la sélection d'une taille de disque, voir Exigences relatives aux machines virtuelles.
8. Configurez tous les champs supplémentaires requis pour votre environnement.
9. Cliquez **Créez**.

Créez l'instance de machine virtuelle

1. Dans le volet de gauche, Moteur de calcul page, **Instances de machines virtuelles**.
2. Cliquez **Créer une instance** et effectuez les étapes suivantes :
   a) Dans le Nom dans le 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 lieu dans votre zone géographique.
   d) Dans le Configuration de la machine section, sélectionnez **Usage général** pour la famille de machines.

      Pour plus d'informations sur la sélection d'un type de machine, voir Exigences relatives aux machines virtuelles.
   e) Dans le Disque de démarrage section, cliquez sur **Changement**.
   f) Cliquez **Disques existants**.
   g) À partir du Disque dans la liste déroulante, sélectionnez le disque que vous avez créé précédemment.
   h) Cliquez **Sélectionnez**.
3. Cliquez **Options avancées**.
4. Cliquez **Réseautage**.
5. Dans le champ Balises réseau, saisissez les noms de balises suivants, en les séparant par un espace :
   - `serveur https`
   - `serveur http`
   - `dns`
   - `ssh-all`



> **Important:** Les balises réseau sont requises pour appliquer les règles de pare-feu à l'instance ExtraHop. Si aucune règle de pare-feu n'autorise ce trafic, vous devez créer les règles. Pour plus d'informations, voir https://cloud.google.com/vpc/docs/using-firewalls.

6. Dans le Interfaces réseau section, cliquez sur l' interface de gestion.
   a) À partir du Réseau dans la 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 management et l'interface de capture de données doivent se trouver sur des réseaux de cloud privé virtuel (VPC) différents.

   a) À partir du Réseau dans la liste déroulante, sélectionnez le réseau qui reflétera le trafic vers le système ExtraHop.
   b) À partir du Sous-réseau liste déroulante, sélectionnez votre sous-réseau réseau.
   c) À partir du IPv4 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 de gauche, Moteur de calcul page, cliquez **Groupes d'instances**.
2. Cliquez **Créer un groupe d'instances**.
3. Cliquez **Nouveau groupe d'instances non géré**.
4. Dans le Nom dans le champ, saisissez le nom d'un groupe d'instances.
5. À partir du Réseau dans la liste déroulante, sélectionnez le réseau auquel l'instance peut accéder.
6. À partir du Sous-réseau dans la liste déroulante, sélectionnez votre sous-réseau réseau.
7. À partir du Sélectionnez une machine virtuelle dans la liste déroulante, sélectionnez votre sonde.
8. Cliquez **Créez**.

Création d'un équilibreur de charge

1. Dans le menu de navigation, cliquez sur **Services réseau** > **équilibrage de charge**.

   Note: Si le Services réseau le menu ne figure pas dans votre menu de navigation, cliquez sur **Plus de produits**.
2. Cliquez **Créer un équilibreur de charge**.
3. Dans le Équilibreur de charge réseau (UDP/protocoles multiples) section, cliquez sur **Démarrer la configuration**.
4. En dessous Sélectionnez un type d'équilibreur de charge, cliquez **Équilibreur de charge UDP**.
5. En dessous Accès à Internet ou interne uniquement, sélectionnez **Uniquement entre mes machines virtuelles**.
6. En dessous Type de backend, conservez la valeur par défaut (Backend Service).
7. Cliquez **Continuer**.
8. Dans le Nom de l'équilibreur de charge dans le champ, saisissez le nom d'un équilibreur de charge.
9. À partir du Région dans la liste déroulante, sélectionnez votre région géographique.
10. À partir du Réseau dans la liste déroulante, sélectionnez votre réseau.
11. Dans le Backends section, à partir de la Groupe d'instances dans la liste déroulante, sélectionnez votre groupe d'instances.
12. Cliquez **Bilan de santé** puis cliquez sur **Créer un bilan de santé**.
13. Dans le Nom dans le champ, saisissez le nom du bilan de santé.

14. À partir du Protocole liste déroulante, sélectionnez **TCP**.
15. Dans le Port champ, type 443.
16. Cliquez **Enregistrer**.

Création d'une politique de mise en miroir du trafic

1. Dans le menu de navigation, cliquez sur **Réseau VPC** > **Mise en miroir de paquets**.
2. Cliquez **Créer une politique**.
3. Dans le Nom de la politique champ, saisissez un nouveau nom de politique.
4. À partir du Région dans la liste déroulante, sélectionnez votre région géographique.
5. Cliquez **Continuer**.
6. Sélectionnez **La source en miroir et la destination du collecteur se trouvent sur le même réseau VPC** .
7. À partir du Réseau dans la liste déroulante, sélectionnez le réseau VPC.
8. Cliquez **Continuer**.
9. Sélectionnez le **Sélectionnez un ou plusieurs sous-réseaux** case à cocher.
10. À partir du Sélectionnez un sous-réseau dans la liste déroulante, cochez la case à côté de votre sous-réseau.
11. Cliquez **Continuer**.
12. Cochez la case à côté de l'instance de machine virtuelle.
13. Cliquez **Continuer**.
14. À partir du **Destination du collectionneur** liste déroulante. Sélectionnez l'équilibreur de charge que vous avez créé précédemment.
15. Cliquez **Continuer**.
16. Sélectionnez **Afficher tout le trafic en miroir (par défaut)**.
17. Cliquez **Soumettre**.

Configuration de la sonde

Avant de commencer
Avant de pouvoir configurer la sonde, vous devez avoir déjà configuré une adresse IP de gestion.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

   Le nom de connexion par défaut est `setup` et le mot de passe est l'ID de l'instance de machine virtuelle.
2. Acceptez le contrat de licence, puis connectez-vous.
3. 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.

Prochaines étapes
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.

Configuration de la découverte des équipements L3

Vous devez configurer le système ExtraHop pour détecter et suivre les appareils locaux et distants en fonction de 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 sur **Capturez**.
3. Cliquez **Découverte d'appareils**.
4. Dans le Découverte d'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 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**.