Liste de contrôle après le déploiement des capteurs et des consoles

Publié: 2025-03-28

Après avoir déployé un ExtraHop sonde ou console, connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin` et configurez les paramètres suivants. Reportez-vous à la section du Guide de l'interface utilisateur d'ExtraHop spécifié dans chaque action ci-dessous, sauf indication contraire.

Procédures requises

Vous devez suivre ces procédures pour déployer complètement votre système ExtraHop.

DNS

Le DNS permet la résolution des noms de domaine. Vérifiez que vous avez configuré des serveurs DNS. Accédez au CLI interface avec un terminal ou accédez à l'interface d'administration > Connectivité page pour modifier ou définir les adresses IP DNS. Vous pouvez définir des adresses IP DNS à l'aide du panneau avant ou Dirac interface sur les appareils physiques.

Nom d'hôte du système

Définissez un nom d'hôte système unique afin que la console ExtraHop puisse rétablir la connectivité en cas de modification de l'adresse IP. Si l'enregistrement A est « hq-eda01.acme.org », votre nom d'hôte doit être « hq-eda01 ».

Mot de passe

Maintenez la sécurité du système après la période d'évaluation. Modifiez le mot de passe par défaut. Pour plus d'informations, consultez le FAQ sur les comptes utilisateurs par défaut. Nous vous recommandons de créer un compte d'administrateur secondaire avec des informations d'identification distinctes à titre de sauvegarde au cas où les informations d'identification de l'administrateur principal seraient perdues.

NTP et fuseau horaire

Le temps est essentiel dans le système ExtraHop, en particulier lors de la corrélation d'événements avec des métriques et des journaux temporels. Vérifiez que les paramètres NTP sont corrects pour votre infrastructure, testez les paramètres et synchronisez le protocole NTP. Le fuseau horaire correct est essentiel pour exécuter les rapports planifiés au bon moment. Assurez-vous que le fuseau horaire du système ExtraHop est correct. Pour plus d'informations, voir Configurer l'heure du système.

Appliquer une licence

Vous devez appliquer une clé de produit pour activer et enregistrer votre appareil.

Services cloud

Connectez-vous aux services cloud ExtraHop pour activer les détections et l'accès à distance. Pour plus d'informations, voir Connectez-vous aux services cloud ExtraHop.

Mise à jour du firmware

Le firmware de l'ExtraHop est régulièrement mis à jour avec des améliorations et des défauts résolus. Vérifiez que vous disposez du microprogramme actuel. Pour plus d'informations, voir Mettez à jour le firmware de votre système ExtraHop.

Connecter les appareils

Connectez le console et des capteurs pour tous les magasins de paquets et de disques. Pour plus d'informations, voir Connectez l'EXA 5200 au système ExtraHop et Connecter un stockage des paquets à RevealX Enterprise.

Procédures recommandées

Nous vous recommandons de suivre ces procédures pour optimiser les performances de votre système ExtraHop.

Certificat TLS

Chaque système ExtraHop est livré avec un certificat auto-signé. Si vous avez un déploiement PKI, générez votre propre certificat et téléchargez-le sur chaque système ExtraHop. Pour plus d'informations, consultez le Certificat TLS section.

Enregistrement DNS A

Il est plus facile d'accéder à un système ExtraHop par nom d'hôte que par adresse IP. Créez un A enregistrement dans votre racine DNS (»`exa.yourdomain.local`«) pour chaque système ExtraHop de votre déploiement. Reportez-vous à votre manuel d'administration du DNS.

Authentification et accès à distance

Configurez l'authentification à distance. L'appliance ExtraHop s'intègre à SAML (de préférence pour la console), LDAP, RAYON, et TACACS+. Restreignez l' accès à distance depuis l'Internet public à l'aide d'un VPN d'entreprise, d'un proxy sensible à l'identité (IAP) ou d'une autre méthode.

Journalisation des audits

Le système ExtraHop peut envoyer des événements à un collecteur Syslog distant. Pour plus d'informations, consultez le Envoyer les données du journal d'audit à un serveur Syslog distant.

Notifications du système

Le système ExtraHop peut envoyer des e-mails lorsqu'il détecte des problèmes. Créez un groupe d'e-mails pour recevoir des notifications. Pour plus d'informations, voir Configuration d'un groupe de notifications par e-mail.

Chiffrement des disques

Activez la sécurité des unités de stockage pour assurer le chiffrement des disques virtuels. Pour plus d'informations, voir Configuration des disques à chiffrement automatique (SED).

Localités du réseau

Classez les adresses IP non conformes à la RFC1918 comme faisant partie de votre réseau interne. Pour plus d'informations, voir Spécifier une localité du réseau.

Paramètres de réglage

Contribuez à améliorer la qualité et la précision des détections basées sur des règles en ajoutant des paramètres de réglage. Pour plus d'informations, voir Spécifier les paramètres de réglage pour les détections et les métriques.

Analyse avancée

Ciblez des groupes d'équipements ou des groupes d'activités spécifiques pour une Analyse avancée selon les besoins, en fonction de leur importance pour votre réseau. Pour plus d'informations, voir Priorités d'analyse.

Configurer le déchiffrement du contrôleur de domaine

Le système ExtraHop peut être configuré pour récupérer et stocker les clés de domaine d'un ou de plusieurs contrôleurs de domaine. Lorsque le système observe un trafic chiffré qui correspond aux clés mises en cache, tout le trafic crypté Kerberos du domaine est déchiffré pour les protocoles pris en charge. Pour plus d'informations, voir Déchiffrez le trafic de domaine à l'aide d'un contrôleur de domaine Windows.

Personnalisations et sauvegarde de la banque de données

Créez une sauvegarde du système avant de procéder à la mise à niveau du microprogramme ou avant d'apporter une modification majeure à votre environnement. Pour plus d'informations, voir Sauvegarder une sonde ou une console.

Dirac

Chaque appliance ExtraHop physique possède un Dirac port, similaire à iLO ou KVM over Ethernet. Connectez et configurez le port iDRAC. Pour plus d'informations, voir Configuration de la console d'accès à distance iDRAC.

Déchiffrez le trafic TLS avec le partage secret

Déchiffrez le trafic TLS de vos serveurs Linux et Windows. Pour plus d'informations, voir Installation du redirecteur de clés de session ExtraHop sur un serveur Linux et Installation du redirecteur de clés de session ExtraHop sur un serveur Windows. Vous pouvez également partager les clés de session avec votre système ExtraHop via votre Équilibreur de charge F5 avec Perfect Forward Secrecy (PFS).

Procédures facultatives

Envisagez de suivre ces procédures si vous souhaitez personnaliser davantage votre système ExtraHop .

Activer le lecteur de disque PPCAP (Precision Packet Capture)

La capture de paquets vous permet de collecter, de stocker et de récupérer des paquets de données à partir de votre trafic réseau. Si vous disposez d'un disque de capture de paquets de précision, consultez Configuration de la capture de paquets.

SMTP

Le système ExtraHop peut envoyer des alertes par e-mail et des notifications relatives à l'état du système. Configurez et testez les notifications. Pour plus d'informations, voir Configurer les paramètres de messagerie pour les notifications.

Activer le lecteur de disque PPCAP (Precision Packet Capture)

La capture de paquets vous permet de collecter, de stocker et de récupérer des paquets de données à partir de votre trafic réseau. Si vous disposez d'un disque de capture de paquets de précision, consultez Configuration de la capture de paquets.

Renseignements sur les menaces

Configurez les paramètres des renseignements sur les menaces pour identifier les indicateurs de compromission sur votre réseau. Pour plus d'informations, voir Renseignements sur les menaces.

Déchiffrez le trafic TLS avec des clés privées RSA

Déchiffrez le trafic TLS transféré en téléchargeant la clé privée et le certificat de serveur associés à ce trafic. Pour plus d'informations, voir Déchiffrez le trafic TLS avec des certificats et des clés privées.

Configuration du SNMP

Vous pouvez configurer des interruptions SNMP et configurer les paramètres SNMP pour vous informer de certains événements du réseau.