Liste de contrôle après le déploiement des capteurs et des consoles

Publié: 2024-11-04

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.

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.

NTP

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. Pour plus d'informations, voir Configurer l'heure du système.

Fuseau horaire

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.

Authentification à distance

Configurez l'authentification à distance. L'appliance ExtraHop s'intègre à LDAP, RAYON, SAML, et TACACS+.

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.

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.

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.

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.

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.

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.

Chiffrement des disques

Activez la sécurité des unités de stockage pour assurer le chiffrement des disques virtuels (EDA 9300, EDA 10300 et IDS 9380 uniquement). Pour plus d'informations, voir Configuration des disques à chiffrement automatique (SED).

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 Connectez les capteurs et la console au stockage des paquets.

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.

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

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.

Déchiffrer le trafic TLS

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 à l'aide de certificats et de clés privées.

Configuration de la confidentialité avancée parfaite (PFS)

Déchiffrez le trafic TLS de vos serveurs Linux et Windows. Pour plus d'informations, voir Installez le redirecteur de clé de session ExtraHop sur un serveur Linux et Installation du redirecteur de clés de session ExtraHop sur un serveur 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.