

ExtraHop

Checkliste für die Nachverfolgung nach der Bereitstellung

Veröffentlicht: 2024-03-20

Nachdem Sie die ExtraHop Trace-Appliance bereitgestellt haben, melden Sie sich bei den Administrationseinstellungen auf dem ExtraHop-System an über `https://<extrahop-hostname-or-IP-address>/admin` und konfigurieren Sie die folgenden Einstellungen.

Passwort

Sorgen Sie nach dem Testzeitraum für die Systemsicherheit. Ändern Sie das Standardkennwort. Weitere Informationen finden Sie in der [Häufig gestellte Fragen zu Standardbenutzerkonten](#).

NTP

Zeit ist im ExtraHop-System von entscheidender Bedeutung, insbesondere bei der Korrelation von Ereignis mit zeitbasierten Metriken und Protokollen. Stellen Sie sicher, dass die NTP-Einstellungen für Ihre Infrastruktur korrekt sind, testen Sie die Einstellungen und synchronisieren Sie NTP. Weitere Informationen finden Sie unter [Systemzeit konfigurieren](#).

Zeitzone

Die richtige Zeitzone ist wichtig, um geplante Dashboard-Berichte zur richtigen Zeit auszuführen. Stellen Sie sicher, dass das ExtraHop-System die richtige Zeitzone hat. Weitere Informationen finden Sie unter [Systemzeit konfigurieren](#).

Fernauthentifizierung

Richten Sie die Fernauthentifizierung ein. Das ExtraHop-System lässt sich integrieren mit [LDAP](#), [RADIUS](#), und [TACACS+](#) für die Fernintegration.

Firmware-Aktualisierung

Die ExtraHop-Systemfirmware wird häufig mit Verbesserungen aktualisiert und Fehler behoben. Stellen Sie sicher, dass Sie über die aktuelle Firmware verfügen. Weitere Informationen finden Sie unter [Aktualisieren Sie die Firmware auf Ihrem ExtraHop-System](#).

Audit-Protokollierung

Das ExtraHop-System kann Ereignisse an einen entfernten Syslog-Collector senden. Weitere Informationen finden Sie in der [Audit-Log-Daten an einen Remote-Syslog-Server senden](#).

SMTP

Das ExtraHop-System kann Benachrichtigungen und Benachrichtigungen zur Systemintegrität per E-Mail versenden. Benachrichtigungen einrichten und testen. Weitere Informationen finden Sie unter [E-Mail-Einstellungen für Benachrichtigungen konfigurieren](#).

Systembenachrichtigungen

Das ExtraHop-System kann E-Mail-Benachrichtigungen senden, wenn Festplattenfehler erkannt werden. Fügen Sie E-Mail-Adressen hinzu, um Benachrichtigungen zum Systemstatus zu erhalten. Weitere Informationen finden Sie in der [Benachrichtigungen](#).

iDRAC

Jede physische ExtraHop-Appliance hat eine iDRAC Port, ähnlich wie iLO oder KVM over Ethernet. Stellen Sie eine Verbindung zum iDRAC-Port her und konfigurieren Sie ihn. Weitere Informationen finden Sie unter [Konfiguration der iDRAC Remote Access Console](#).

SSL Zertifikat

Jedes ExtraHop-System wird mit einem selbstsignierten Zertifikat geliefert. Wenn Sie eine PKI-Implementierung haben, generieren Sie Ihr eigenes Zertifikat und laden Sie es auf jedes ExtraHop-

System hoch. Weitere Informationen finden Sie in der [SSL-Zertifikat](#) Abschnitt im ExtraHop-Administrationshandbuch.

DNS-A-Datensatz

Es ist einfacher, über den Hostnamen auf eine Trace-Appliance zuzugreifen als über die IP-Adresse. Erstelle eine `A` Datensatz in deinem DNS Wurzel ("`eta.yourdomain.local`„) für jede Trace-Appliance in Ihrer Bereitstellung. Schlagen Sie in Ihrem DNS-Administrationshandbuch nach.

Cloud-Dienste

Stellen Sie eine Verbindung zu ExtraHop Cloud Services her, um den Fernzugriff zu aktivieren. Weitere Informationen finden Sie unter [Stellen Sie eine Verbindung zu ExtraHop Cloud Services her](#).