Systembenachrichtigungen an einen Remote-Syslog-Server senden

Veröffentlicht: 2024-08-09

Mit der Syslog-Exportoption können Sie Warnmeldungen von einem ExtraHop-System an jedes Remote-System senden, das Syslog-Eingaben zur Langzeitarchivierung und Korrelation mit anderen Quellen empfängt.

Für jedes ExtraHop-System kann nur ein Remote-Syslog-Server konfiguriert werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Benachrichtigungen**.
3. In der Reiseziel Feld, geben Sie die IP-Adresse des Remote-Syslog-Servers ein.
4. Aus dem **Protokoll** Dropdownliste, wählen **TCP** oder **UDP**.

   Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.
5. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Remote-Syslog-Server ein.

   Der Standardwert ist 514.
6. Klicken Sie **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollte in der Syslog-Logdatei auf dem Syslog-Server ein Eintrag ähnlich dem folgenden angezeigt werden:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Klicken Sie **Speichern**.
8. Optional: Ändern Sie das Format von Syslog-Meldungen.

   Standardmäßig sind Syslog-Meldungen nicht mit RFC 3164 oder RFC 5424 kompatibel. Sie können Syslog-Meldungen jedoch so formatieren, dass sie konform sind, indem Sie die laufende Konfigurationsdatei ändern.
   a) Klicken Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken Sie **Konfiguration bearbeiten**.
   d) Fügen Sie einen Eintrag hinzu unter `syslog_notification`, wo der Schlüssel ist `rfc_compliant_format` und der Wert ist entweder `rfc5424` oder `rfc3164`.

      Das `syslog_notification` Der Abschnitt sollte dem folgenden Code ähneln:

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```
   e) Klicken Sie **Aktualisieren**.
   f) Klicken Sie **Erledigt**.
9. Optional: Ändern Sie die Zeitzone, auf die in den Syslog-Zeitstempeln verwiesen wird.

   Standardmäßig verweisen Syslog-Zeitstempel auf die UTC-Zeit. Sie können Zeitstempel jedoch so ändern, dass sie auf die ExtraHop-Systemzeit verweisen, indem Sie die laufende Konfigurationsdatei ändern.
   a) Klicken Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.

c) Klicken Sie **Konfiguration bearbeiten**.

d) Fügen Sie einen Eintrag hinzu unter `syslog_notification` wo der Schlüssel ist `syslog_use_localtime` und der Wert ist `true`.

Das `syslog_notification` Der Abschnitt sollte dem folgenden Code ähneln:

```
    "syslog_notification": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

e) Klicken Sie **Aktualisieren**.

f) Klicken Sie **Erledigt**.

Nächste Schritte

Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, speichern Sie Ihre Konfigurationsänderungen durch Systemneustart- und Shutdown-Ereignisse, indem Sie die laufende Konfigurationsdatei speichern.