Systembenachrichtigungen an einen Remote-Syslog-Server senden

Veröffentlicht: 2024-04-10

Mit der Syslog-Exportoption können Sie Warnungen 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 Netzwerk-Einstellungen Abschnitt, klicken **Benachrichtigungen**.
3. Geben Sie im Feld Ziel die IP-Adresse des Remote-Syslog-Servers ein.
4. Wählen Sie im Dropdownmenü Protokoll **TCP** oder **UDP**. Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.
5. Geben Sie im Feld Port die Portnummer für Ihren Remote-Syslog-Server ein. Standardmäßig ist dieser Wert auf 514 festgelegt.
6. Klicken **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind. Wenn die Einstellungen korrekt sind, sollten Sie in der Syslog-Log-Datei auf dem Syslog-Server einen Eintrag sehen, der dem folgenden ähnelt:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

7. Klicken **Speichern**.
8. Optional: Ändern Sie das Format von Syslog-Meldungen.

   Standardmäßig entsprechen Syslog-Meldungen nicht RFC 3164 oder RFC 5424. Sie können Syslog-Meldungen jedoch so formatieren, dass sie konform sind, indem Sie die laufende Konfigurationsdatei ändern.

   a) Klicken **Admin**.
   b) Klicken **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken **Konfiguration bearbeiten**.
   d) Füge 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 **Aktualisieren**.
   f) Klicken **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 **Admin**.
   b) Klicken **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken **Konfiguration bearbeiten**.

d) Füge 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 **Aktualisieren**.

f) Klicken **Erledigt**.

Nächste Schritte

Nachdem Sie sich vergewissert haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, behalten Sie Ihre Konfigurationsänderungen bei Systemneustart- und Shutdown-Ereignissen bei, indem Sie die laufende Konfigurationsdatei speichern.