Logs (Günlükler) Yapılandırması

TheHive, çalışan süreç hakkında bilgi kaydetmek için logback kullanır. Logs, /etc/thehive/logback.xml dosyasında yapılandırılır. Bu dosyayı düzenleyin ve değişikliklerinizi uygulamak için hizmeti yeniden yükleyin.

Varsayılan olarak, günlükler /var/log/thehive/ dizininde depolanır. Son günlük dosyasına application.log denir ve eski dosyalar application.%i.log.zip biçiminde sıkıştırılmış bir formatta saklanır.

Log Seviyesini Artırma/Azaltma

Logback, birkaç log seviyesini destekler.

Daha fazla şeyi kaydetmek için kök düzeyini DEBUG (veya TRACE) olarak güncelleyebilirsiniz:

logback.xml

```
<!-- ... -->
<root level="DEBUG">
  <!-- ... -->
</root>
```

Daha az şeyi log kaydetmek için WARN, ERROR veya OFF seviyelerini kullanabilirsiniz.

Log seviyesi, belirli bir kaydedicinin seviyesi değiştirilerek ayrı ayrı da güncellenebilir:

logback.xml

```
<logger name="org.thp" level="DEBUG"/>
```

Docker'da Logs

Docker içindeki konteynerde, günlükleyici varsayılan olarak */etc/thehive/logback.xml* dosyasıyla yapılandırılır ve uygulama stdout'a ve */var/log/thehive/application.log*'a günlükler.

Varsayılan yapılandırmayı değiştirmek isterseniz, kendi logback dosyanızı /etc/thehive/logback.xml'ye bağlayabilirsiniz.

Logback Yapılandırmanızı Hata Ayıklama

Eğer sorunlarınız varsa logback.xml'de debug bayrağını true olarak ayarlayın:

logback.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration debug="true">
```

Bu, uygulama başladığında logback yapılandırmanızı konsola kaydeder.

Log Erişimi Nasıl Oluşturulur

Logback yapılandırmasını değiştirerek, belirli günlükleri uygulamadan başka bir yere yönlendirebilirsiniz. Aşağıda, erişim günlüklerinin *access.log* dosyasına yönlendirildiği ve bir döner dosya stratejisi kullandığı bir örnek bulunmaktadır.

Bu yapılandırmayı uygulamak için, ekleyicileri ve günlükleyicilerin tanımlarını kopyalayın.

logback.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration debug="false">

  <!-- ... other appenders and settings -->

  <appender name="ACCESSFILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <file>/var/log/thehive/access.log</file>
    <rollingPolicy class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
      <fileNamePattern>/var/log/thehive/access.%i.log.zip</fileNamePattern>
      <minIndex>1</minIndex>
      <maxIndex>10</maxIndex>
    </rollingPolicy>
    <triggeringPolicy class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
      <maxFileSize>10MB</maxFileSize>
    </triggeringPolicy>

    <encoder>
      <pattern>%date [%level] from %logger [%traceID] %message%n%xException</pattern>
    </encoder>
  </appender>

  <appender name="ASYNCACCESSFILE" class="ch.qos.logback.classic.AsyncAppender">
    <appender-ref ref="ACCESSFILE"/>
  </appender>
```

```
    <logger name="org.thp.scalligraph.AccessLogFilter">
        <appender-ref ref="ASYNCACCESSFILE" />
    </logger>
    <logger name="org.thp.scalligraph.controllers.Entrypoint">
        <appender-ref ref="ASYNCACCESSFILE" />
    </logger>

    <root level="INFO">
        <!-- other appender-refs ... -->
    </root>

</configuration>
```

Log'lar syslog'a Nasıl Gönderilir

Bir SyslogAppender eklemeniz gerekecektir.

logback.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration debug="false">

    <!-- ... other appenders and settings -->

    <appender name="SYSLOG" class="ch.qos.logback.classic.net.SyslogAppender">
        <syslogHost>remote_host</syslogHost>
        <facility>AUTH</facility>
        <suffixPattern>[%thread] %logger %msg</suffixPattern>
    </appender>

    <root level="INFO">
        <appender-ref ref="SYSLOG" />
        <!-- other appender-refs ... -->
    </root>
```

Sınırlamalar: Resmi syslog uygulayıcısı günlükleri yalnızca UDP üzerinden bir sunucuya gönderebilir. TCP ve TLS kullanamaz

---

Revision #2
Created 12 April 2024 21:33:12 by Güldeniz Akca
Updated 13 April 2024 15:03:30 by Güldeniz Akca