### 연결 문제 진단

#### 웹 관리 콘솔에서 전달 노드 접속 상태가 회색으로 표시됨

방화벽 정책 문제 진단

먼저 분석 서버에서 전달 서버의 웹 서버에 접속 가능한지 확인해야 합니다. 분석 서버의 로그프레소 셸에 로그인한 후에 아래와 같이 전달 서버 IP 주소와 웹 서버 포트를 입력하여 접속 가능 여부를 확인합니다.

logpresso> tcpscan x.x.x.x 8443trying to connect /x.x.x.x:8443timeout

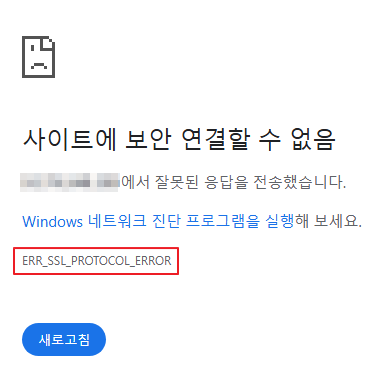
tcpscan 명령 시 일정 시간 후에 timeout이 표시된다면 분석 서버에서 전달 서버에 이르는 통신 경로에 위치한 모든 방화벽의 정책을 재확인합니다.

not opened: Connection refused 메시지가 표시되는 경우에는 웹 서버 포트가 열리지 않은 것이므로, 전달 서버의 로그프레소 셸에서 httpd.bindings 명령어를 실행하여 포트 설정을 재확인합니다. 포트가 열리지 않은 경우 설치 단계에 따라 다시 진행합니다.

SSL 인증서 문제 진단

opened가 표시되는데 여전히 웹 관리 콘솔에서 전달 노드 접속 상태가 회색으로 표시된다면, SSL 인증서 문제이거나 정책 동기화 암호가 잘못 지정된 경우입니다.

운영 단말의 웹 브라우저에서 전달 서버의 8443 포트에 접속 시도했을 때 아래와 같이 ERR\_SSL\_PROTOCOL\_ERROR가 표시된다면 인증서 문제입니다.



전달 서버의 웹 서버 인증서 문제인 경우에는 아래의 사항을 재점검합니다:

* md5sum 명령어를 이용하여 인증서 파일의 해시가 분석 서버의 파일과 동일한지 검증합니다.
* 인증서 파일의 소유자 및 그룹이 logpresso가 맞는지 확인합니다.
* keystore.unregister, keystore.register, httpd.close, httpd.openSsl 단계를 다시 진행합니다.

정책 동기화 암호 문제 진단

전달 서버의 엔터프라이즈 웹 관리 콘솔 화면이 정상적으로 표시된다면, 노드 추가 시 설정했던 계정, 암호를 이 화면에서 입력하여 정상적으로 로그인 가능한지 확인합니다. 만약 로그인이 불가능하다면 전달 서버의 로그프레소 셸에서 dom.resetPassword localhost root 명령을 수행하여 암호를 초기화하고, 웹 관리콘솔의 클러스터 메뉴에서 노드 암호를 재설정합니다.

#### 전달 서버에서 분석 서버 RPC 접속에 실패함

RPC 연결 상태 확인

전달 서버의 로그프레소 셸에서 아래 명령어를 실행하여 분석 서버 RPC 포트에 정상적으로 접속되었는지 확인할 수 있습니다.

logpresso> forwarder.connectionsConnections--------------------[control\_1] id=1317075310, peer=(39c2dd55-5bb5-4497-a327-ee6f8cae9ad9, /x.x.x.x:7140), trusted level=Low, ssl=true, props={phase=post\_hello, ping\_failure=0, type=command}

위와 같이 분석 서버 IP 주소와 관련된 RPC 연결이 표시되지 않는 경우, 방화벽 정책 문제이거나 TLS 상호 인증에 사용되는 인증서의 문제일 수 있습니다.

방화벽 정책 문제 진단

먼저 전달 서버의 로그프레소 셸에서 아래와 같이 네트워크 통신이 방화벽으로 차단되지 않는지 검증합니다.

logpresso> tcpscan [분석서버 IP] 7140trying to connect /x.x.x.x:7140timeout

만약 위와 같이 일정 시간 후에 timeout이 출력된다면 전달 서버에서 분석 서버에 이르는 통신 경로에 위치한 모든 방화벽의 정책을 재확인합니다.

SSL 인증서 문제 진단

전달 서버의 로그프레소 셸에서 logger.tail 명령어를 실행하거나, /opt/logpresso/log/araqne.log 파일을 조회하여 데몬 로그를 확인할 수 있습니다.

**인증서 암호 오류**

아래와 같이 keystore password was incorrect 오류가 발생하는 경우에는 인증서 암호가 잘못된 것이므로, 로그프레소 셸에서 keystore.unregister, keystore.register 명령어를 이용하여 올바른 암호와 함께 인증서를 다시 등록합니다.

[2025-01-30 09:24:10.812] WARN (KeyStoreManagerImpl) - getKeyStore() error:java.io.IOException: keystore password was incorrect at java.base/sun.security.pkcs12.PKCS12KeyStore.engineLoad(PKCS12KeyStore.java:2116) at java.base/sun.security.util.KeyStoreDelegator.engineLoad(KeyStoreDelegator.java:222) at java.base/java.security.KeyStore.load(KeyStore.java:1479) at org.araqne.keystore.KeyStoreManagerImpl.getKeyStore(KeyStoreManagerImpl.java:298) at org.araqne.keystore.KeyStoreManagerImpl.getKeyManagerFactory(KeyStoreManagerImpl.java:414) at org.araqne.rpc.RpcKeyStoreManagerImpl.\_\_M\_getKeyManagerFactory(RpcKeyStoreManagerImpl.java:62) at org.araqne.rpc.RpcKeyStoreManagerImpl.getKeyManagerFactory(RpcKeyStoreManagerImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_M\_connect(ConnectionWatchdogImpl.java:216) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.connect(ConnectionWatchdogImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_M\_checkConnections(ConnectionWatchdogImpl.java:171) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.checkConnections(ConnectionWatchdogImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_M\_checkNow(ConnectionWatchdogImpl.java:149) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.checkNow(ConnectionWatchdogImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_M\_run(ConnectionWatchdogImpl.java:123) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.run(ConnectionWatchdogImpl.java) at java.base/java.lang.Thread.run(Thread.java:829)Caused by: java.security.UnrecoverableKeyException: failed to decrypt safe contents entry: javax.crypto.BadPaddingException: Given final block not properly padded. Such issues can arise if a bad key is used during decryption. ... 16 more

**신뢰할 수 없는 인증서 오류**

아래와 같이 No trusted certificate found 오류가 발생하는 경우에는 분석 서버에서 발급한 인증서가 아닌 최초 데몬 시작 시 자동 생성된 인증서가 사용된 것이므로 인증서 파일 복사부터 키스토어 등록 단계까지 다시 진행합니다.

[2025-01-30 09:28:14.623] ERROR (ConnectionWatchdogImpl) - logpresso-sentry: failed to connect, closing connection (No trusted certificate found)[2025-01-30 09:28:14.624] ERROR (RpcHandler) - araqne rpc: ssl handshake exception from x.x.x.x:7140, channel 2ca2e90a (No trusted certificate found)