로그프레소 전달 서버 운영 가이드

## 개요

### 전달 서버 기능

#### 개요

로그프레소 전달 서버는 로그프레소 클러스터에 속한 수집 서버나 분석 서버에 데이터를 전달하거나, 외부 데이터 시스템으로 데이터를 전달합니다.

로그프레소 센트리도 데이터를 전달하는 기능을 제공하지만, 센트리는 관리 대상 서버에 설치되는 용도이기 때문에 최소한의 시스템 자원을 사용하도록 설계되어 있으며 수집에 관련된 최소한의 기능만을 제공합니다. 반면 전달 서버는 독립적인 머신으로 구성되며 앱 설치를 포함한 서버의 기능을 제공합니다.

특히 사용자 네트워크에 위치한 장비에서 로그프레소 클라우드 인스턴스에 Syslog를 전송하는 경우에는 인터넷 구간에서 평문 노출을 방지하고 UDP 패킷 유실을 최소화하기 위하여 사용자 네트워크에 전달 서버를 설치하여 로그를 전달해야 합니다.

#### 기능 비교

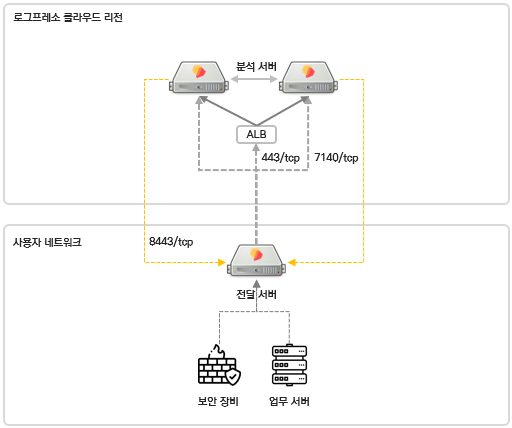
아래 표는 센트리와 전달 서버 기능을 대비하여 요약 설명합니다:

|  |  |  |
| --- | --- | --- |
| 기능 | 센트리 | 전달 서버 |
| 시스템 자원 | 최소 사용 | 전체 사용 |
| TLS 암호화 통신 | 지원 | 지원 |
| 실시간 압축 전송 | 지원 | 지원 |
| 데이터 수집 | 지원 | 지원 |
| 데이터 파싱 | 미지원 | 미지원 |
| 데이터 필터링 | 지원 | 지원 |
| 내부 데이터 중계 | 미지원 | 지원 |
| 외부 시스템 전달 | 미지원 | 지원 |
| 쿼리 실행 | 미지원 | 지원 |
| 앱 설치 | 미지원 | 지원 |
| 고가용성 구성 | 미지원 | 지원 |
| 자동 부하 분산 | 미지원 | 지원 |

### 배포 구성

전달 서버를 사용하는 환경과 시나리오에 따라 아래와 같이 구성합니다.

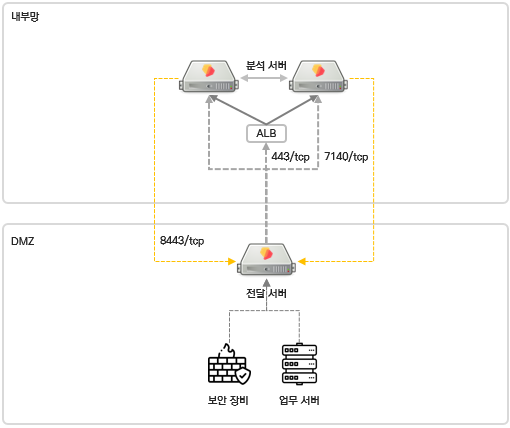
#### 로그프레소 클라우드



이 시나리오에서는 로그프레소 전달 서버가 로그프레소 클러스터와 물리적으로 분리된 외부 환경에 위치합니다. 로그프레소 전달 서버는 방화벽으로 보호되는 사용자 네트워크 내부에 설치되며, 보안 장비에서 직접 로그를 수신하거나 업무 서버에 설치된 로그프레소 센트리에서 로그를 수신하여 로그프레소 클라우드로 전달합니다.

전달 서버 구성 시 로그프레소 클라우드 인스턴스의 공인 IP 주소와 ALB 공인 IP 주소를 전달받아 사용자 네트워크의 방화벽에서 인바운드 NAT 정책과 아웃바운드 허용 정책을 설정해야 합니다.

#### 로그프레소 소나



이 시나리오는 인터넷 통신이 가능한 DMZ와 내부망이 분리된 온프레미스 구성입니다. 로그프레소 클러스터는 외부에서 접근할 수 없는 내부망에 설치되며, 전달 서버는 직접 혹은 망연계 장비를 경유하여 분석 또는 수집 서버에 접속합니다.

망연계 장비를 경유하여 접속하는 경우 사전 준비 절을 참고하여 스트림 연계 방식으로 3가지 경로를 허용하도록 설정해야 합니다.

### 시스템 요구사양

전달 서버의 하드웨어 사양은 예상되는 일 수집량과 센트리 접속 수를 기준으로 산정합니다. 통상 일 수집 원본 로그 기준 1TB, 센트리 접속 수 500대를 기준으로 인스턴스를 분할하며, 이중화 기반 고가용성 구성으로 장애에 대비합니다.

|  |  |  |
| --- | --- | --- |
| 항목 | 일 1TB 이하 | 일 2TB 이하 |
| 평균 수집 속도 | 12MB/s | 24MB/s |
| 최대 수집 속도 | 50MB/s | 100MB/s |
| 최대 EPS | 약 10만 | 약 20만 |

* 위 표의 EPS는 평균 500바이트의 로그를 가정합니다.

#### 네트워크 수집 전용

|  |  |  |
| --- | --- | --- |
| 항목 | 일 1TB 이하 | 일 2TB 이하 |
| CPU 클럭 | 2.4GHz | 3GHz |
| CPU 코어 | 4개 | 8개 |
| RAM | 8GB | 16GB |
| 디스크 가용 공간 | 1TB | 2TB |
| AWS 인스턴스 | c5.xlarge | c5.2xlarge |

* HDD 용량은 수집 서버 장애 시 최대 일주일 보관과 85% 압축을 가정합니다.

#### 센트리 관리 및 네트워크 수집

최대 500대까지 센트리 접속이 예상되는 경우에는 아래의 권장 사양을 적용합니다.

|  |  |  |
| --- | --- | --- |
| 항목 | 일 1TB 이하 | 일 2TB 이하 |
| CPU 클럭 | 2.4GHz | 3GHz |
| CPU 코어 | 16개 | 32개 |
| RAM | 64GB | 64GB |
| 디스크 가용 공간 | 1TB | 2TB |

* HDD 용량은 수집 서버 장애 시 최대 일주일 보관과 85% 압축을 가정합니다.

## 설치

### 사전 준비

전달 서버 호스트명 정의

IP 주소 할당

* 전달 서버에 할당할 IP 주소, 넷마스크, 게이트웨이 주소를 확인합니다.

네트워크 로드 밸런서 설정 (고가용성 구성 시)

* 514/udp, 162/udp에 대해 출발지 IP 해시 방식으로 부하 분산합니다.

방화벽 정책 변경: 전달 서버와 수집 서버 또는 분석 서버 간 통신을 허용하도록 방화벽 정책을 변경합니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 출발지 | 목적지 | 포트/프로토콜 | 용도 |
| 운영자 단말 | 전달 서버 | 8443/tcp | 웹 관리콘솔 및 API 점검 |
| 운영자 단말 | 전달 서버 | 22/tcp | SSH 터미널 |
| 보안 장비 | 전달 서버 | 514/udp | Syslog over UDP |
| 보안 장비 | 전달 서버 | 162/udp | SNMP Trap |
| 전달 서버 | 수집 대상 MySQL | 3306/tcp | JDBC 로그 수집 |
| 전달 서버 | 수집 대상 Oracle | 1521/tcp | JDBC 로그 수집 |
| 전달 서버 | 수집 대상 PostgreSQL | 5432/tcp | JDBC 로그 수집 |
| 전달 서버 | 수집 서버 | 7140/tcp | RPC 및 로그 전송 |
| 전달 서버 | 분석 서버 | 7140/tcp | RPC 및 로그 전송 |

전달 서버 장비 반입

* [시스템 요구사항](https://docs.logpresso.com/ko/sonar/4.0/forwarder/ko/sonar/4.0/forwarder/system-requirements)을 참고하여 준비한 베어메탈 또는 가상머신을 예정된 위치에 반입하여 설치합니다.

JDK 다운로드

* 로그프레소 스토어에서 Logpresso JDK 11.0.14.1 버전을 [다운로드](https://logpresso.store/ko/packages/jdk/releases)합니다.

패키지 다운로드

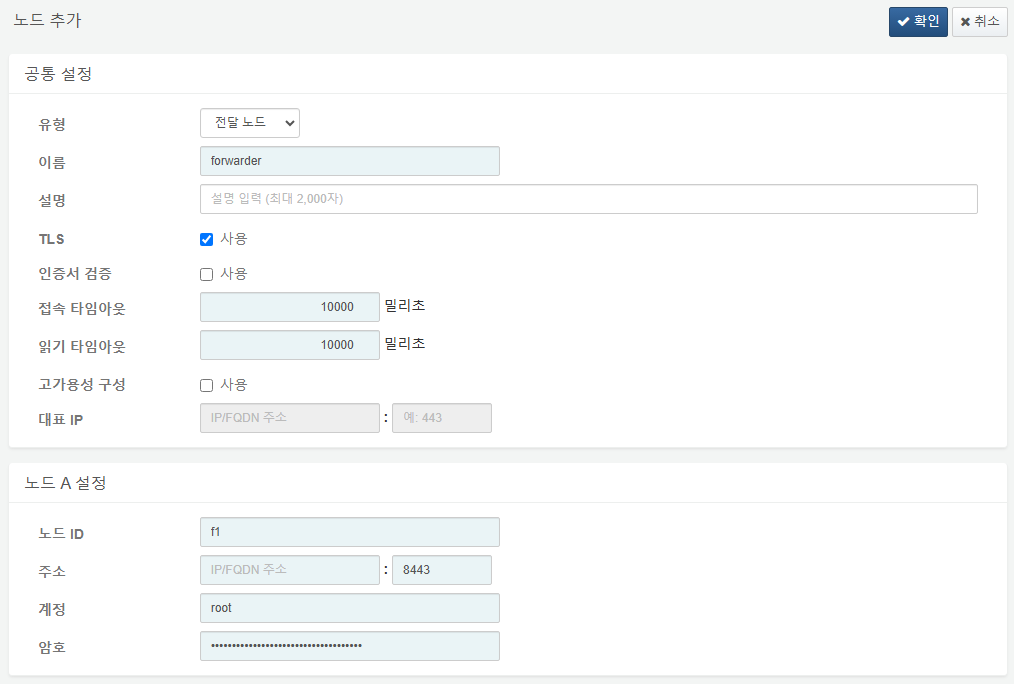
* 로그프레소 스토어에서 분석 서버와 동일한 버전의 패키지를 [다운로드](https://logpresso.store/ko/packages/sonar/releases)합니다.

### 설치

#### 분석 서버 작업

전달 노드 설정 추가

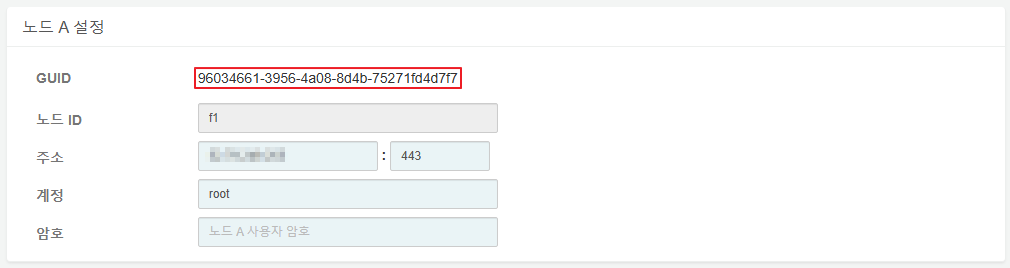
로그프레소 클라우드 또는 로그프레소 소나의 웹 관리 콘솔에서 아래와 같이 전달 노드 설정을 추가합니다.



* 노드 ID: 원격 쿼리 및 수집기의 이름 공간에 사용할 식별자
* 주소
* 로그프레소 클라우드 환경: 사용자 네트워크의 공인 IP 주소 및 NAT 포트
* 로그프레소 소나 환경: 분석 노드의 IP 주소 및 8443 포트
* 계정: root
* 암호: 특수문자를 포함한 16자 이상의 암호를 랜덤하게 생성하여 설정하고 안전한 장소에 보관합니다.

노드 ID는 원격 쿼리 시 사용되는 식별자이므로, 노드 유형과 숫자를 이용하여 짧게 작명하는 것을 권장합니다.

전달 노드 추가 후 노드를 다시 조회하여 GUID를 확인합니다. 이 값은 이후 전달 노드 GUID 설정 단계에서 사용됩니다.



라이선스 노드 추가

분석 서버의 로그프레소 엔터프라이즈 관리 콘솔에서 시스템 설정 > 라이센스 관리 메뉴로 이동하여 새 노드 추가를 클릭하고 이전 단계와 동일 정보를 입력하여 추가합니다. 분석 서버가 2대 이상인 경우 모든 노드에서 설정합니다.



정책 동기화 암호 확인

분석 서버의 로그프레소 셸에서 정책 동기화 암호를 확인합니다.

logpresso> logdb.console rootpassword?

클러스터 노드 추가를 처음 진행하는 경우에는 분석 서버에서 아래와 같이 암호를 재설정합니다.

logpresso> dom.resetPassword localhost rootNew Password:

암호화 키 및 인증서 복사

분석 서버의 로그프레소 셸에 로그인하여 암호화 키를 조회합니다.

$ ssh -p7022 root@localhost Logpresso SNR-4.0.2409.1 (build 20241213) on Araqne Core 4.0.2logpresso@control1 logpresso> sonar.cipherKeyCIPHER\_KEY

암호화 키와 아래 인증서 파일을 다운로드하여 전달 서버에 업로드합니다.

* /data/logpresso-data/logpresso-ca/certs/ca.jks
* /data/logpresso-data/logpresso-ca/certs/base.pfx
* /data/logpresso-data/logpresso-ca/certs/sentry.pfx
* /data/logpresso-data/logpresso-ca/certs/storage.pfx
* /data/logpresso-data/logpresso-ca/certs/web.pfx

로그프레소 클라우드는 로그프레소 지원 포탈(https://support.logpresso.com)에 티켓을 열어서 요청하세요.

#### 운영체제 설치

* Rocky 9.4 이상의 리눅스 배포판을 설치합니다.
* 운영체제 파티션과 데이터 파티션을 분리하여 구성합니다.
* 데이터 파티션은 /data 경로에 마운트합니다.
* 데이터 파티션은 향후 증설을 고려하여 LVM으로 구성합니다.
* 필수 패키지를 설치합니다.
* $ sudo dnf -y install unzip vim net-tools wget firewalld

#### 운영체제 설정

호스트명 설정

전달 서버의 호스트명을 설정합니다.

$ sudo hostnamectl set-hostname LP-FORWARDER1

NTP 활성화

chrony 서비스가 부팅 시 자동으로 시작되도록 설정하고 즉시 시작합니다.

$ sudo systemctl enable chronyd$ sudo systemctl start chronyd

아래 명령어를 실행하면 즉시 시간을 동기화 할 수 있습니다.

$ sudo chronyc -a makestep

SELinux 비활성화

/etc/selinux/config 파일에서 SELINUX 항목을 disabled로 변경합니다.

# This file controls the state of SELinux on the system.# SELINUX= can take one of these three values:# enforcing - SELinux security policy is enforced.# permissive - SELinux prints warnings instead of enforcing.# disabled - No SELinux policy is loaded.SELINUX=permissive # 이 부분을 변경한 후 저장

리눅스 셸에서 관리자 권한으로 아래 명령어를 실행하여 현재 SELINUX 모드를 변경합니다.

# setenforce 0

아래 명령어를 실행하여 현재 SELINUX 동작 모드가 비활성화 상태인지 확인합니다.

# getenforcePermissive

호스트 방화벽 설정

리눅스 셸에서 관리자 권한으로 아래 명령어를 실행하여 호스트 방화벽에서 로그프레소 전달 서버에 필요한 TCP 및 UDP 포트를 개방합니다.

# systemctl enable firewalld# systemctl start firewalld# firewall-cmd --permanent --add-port=8443/tcp# firewall-cmd --permanent --add-port=7140/tcp# firewall-cmd --permanent --add-port=514/udp# firewall-cmd --permanent --add-port=162/udp# firewall-cmd --reload

이어서 아래 명령어를 실행하여 방화벽 설정이 정상적으로 반영되었는지 확인합니다.

# firewall-cmd --list-ports

각 포트의 용도는 아래와 같습니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 프로토콜 | 포트 | 클라이언트 | 용도 |
| TCP | 8443 | 로그프레소 분석 서버 | 접속 앱 설치 및 원격 쿼리 실행 |
| TCP | 7140 | 로그프레소 센트리 | 센트리 원격 관리 및 로그 수집 |
| UDP | 514 | 방화벽 등 어플라이언스 | Syslog 수집 |
| UDP | 162 | 방화벽 등 어플라이언스 | SNMP Trap 수집 |

소켓 버퍼 및 메모리 맵 설정

/etc/sysctl.conf 파일 끝에 아래 항목을 추가합니다.

net.core.rmem\_default = 52428800net.core.rmem\_max = 52428800net.ipv4.udp\_rmem\_min = 8192net.ipv4.ipfrag\_high\_thresh = 16777216vm.max\_map\_count = 10000000

각 항목의 의미는 아래와 같습니다:

|  |  |  |  |
| --- | --- | --- | --- |
| 변수 | 설명 | 기본값 | 설정값 |
| net.core.rmem\_default | 소켓의 기본 수신 버퍼 크기 | 212992 | 52428800 |
| net.core.rmem\_max | 소켓의 최대 수신 버퍼 크기 | 212992 | 52428800 |
| net.ipv4.udp\_rmem\_min | UDP 소켓의 최소 수신 버퍼 크기 | 4096 | 8192 |
| net.ipv4.ipfrag\_high\_thresh | IP 패킷 재조립 버퍼 최대 크기 설정 | 4194304 | 16777216 |
| vm.max\_map\_count | 가상 메모리 맵핑 최대 허용 수 | 65530 | 10000000 |

파일 수정 완료 후 관리자 권한으로 아래 명령어를 실행하여 커널 설정을 변경합니다.

# sysctl -p

이어서 아래 명령어를 실행하여 커널에 의도한대로 설정이 반영되었는지 확인합니다.

# sysctl -a

진단 도구 권한 부여

리눅스 셸에서 관리자 권한으로 visudo 명령어를 실행하여 아래와 같이 추가하고 저장 후 종료합니다.

%logpresso     ALL=(ALL)       NOPASSWD: /opt/logpresso/java/jdk-11.0.14.1-jemalloc/bin/jstack %logpresso     ALL=(ALL)       NOPASSWD: /opt/logpresso/java/jdk-11.0.14.1-jemalloc/bin/jmap %logpresso     ALL=(ALL)       NOPASSWD: /usr/sbin/arping %logpresso     ALL=(ALL)       NOPASSWD: /usr/bin/netstat %logpresso     ALL=(ALL)       NOPASSWD: /usr/sbin/ifconfig %logpresso     ALL=(ALL)       NOPASSWD: /usr/sbin/tcpdump Defaults:logpresso    !requiretty

리소스 제한 완화 설정

/etc/security/limits.conf 파일 끝에 아래 내용을 추가합니다.

logpresso soft nofile 126488logpresso hard nofile 126488logpresso soft nproc 126488logpresso hard nproc 126488

nofile은 동시에 열 수 있는 파일의 최대 수, nproc은 최대 스레드의 수와 관련되어 있습니다.

#### JDK 및 전달 서버 패키지 파일 업로드

사전 준비 단계에서 다운로드한 JDK 및 전달 서버 패키지를 업로드합니다.

* jdk-11.0.14.1-jemalloc-signed.tar.gz
* logpresso-SNR-4.0.2409.1-u3081.zip

#### JDK 및 전달 서버 패키지 설치

리눅스 셸에서 관리자 권한으로 아래 명령어를 실행하여 JDK와 전달 서버 패키지를 설치합니다.

# mkdir -p /opt/logpresso# mkdir -p /data/logpresso-data# cp /home/rocky/jdk-11.0.14.1-jemalloc-signed.tar.gz /opt/logpresso# cp /home/rocky/logpresso-SNR-4.0.2409.1-u3081.zip /opt/logpresso# cd /opt/logpresso# tar zxvf jdk-11.0.14.1-jemalloc-signed.tar.gz# unzip logpresso-SNR-4.0.2409.1-u3081.zip# ln -s /opt/logpresso/jdk-11.0.14.1-jemalloc /opt/logpresso/jre# export JAVA\_HOME=/opt/logpresso/jre# /opt/logpresso/logpresso install config# /opt/logpresso/logpresso install server# chown -R logpresso:logpresso /opt/logpresso# chown -R logpresso:logpresso /data/logpresso-data

#### 전달 서버 설정

/opt/logpresso/etc/logpresso.conf 파일에서 아래 항목을 변경합니다.

JAVA\_HOME="/opt/logpresso/jdk11.0.14.1-jemalloc"MIN\_HEAP\_SIZE=4GMAX\_HEAP\_SIZE=4GMAX\_DIRECT\_MEM\_SIZE=1GLOGKEEPDAY=30DATADIR="/data/logpresso-data"SSH\_OPEN="enabled"

각 설정 항목은 아래와 같은 용도로 사용됩니다.

|  |  |
| --- | --- |
| 변수 이름 | 설명 |
| JAVA\_HOME | JDK를 설치한 절대 경로 |
| MIN\_HEAP\_SIZE | JVM 힙 최소 크기 |
| MAX\_HEAP\_SIZE | JVM 힙 최대 크기 |
| MAX\_DIRECT\_MEM\_SIZE | JVM 다이렉트 메모리 버퍼 최대 크기 |
| LOGKEEPDAY | araqne.log 파일 보관 일수 |
| DATADIR | 로그프레소 데이터 보관 위치의 절대 경로 |
| SSH\_OPEN | 로그프레소 셸 활성화 여부 |

#### 전달 서버 시작

# systemctl start logpresso

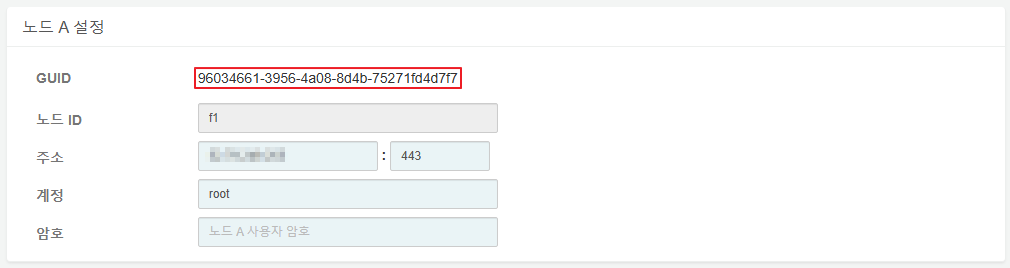
#### 접속 설정

아래 명령어를 입력하여 로그프레소 셸에 진입합니다. 최초 설치 시 로그프레소 셸의 기본 암호는 araqne이며, 반드시 기본 암호를 변경해야 합니다. 프롬프트가 logpresso> 형식으로 바뀌면 정상적으로 접속된 것입니다.

$ ssh -p7022 root@localhost The authenticity of host '[localhost]:7022 ([127.0.0.1]:7022)' can't be established.RSA key fingerprint is SHA256:7gTBAfupl+kkGeNWMJVELkzYCLLZ/13bsgKzR+b3aeU.This key is not known by any other namesAre you sure you want to continue connecting (yes/no/[fingerprint])? yesWarning: Permanently added '[localhost]:7022' (RSA) to the list of known hosts.root@localhost's password:Please change the default password.New password:Retype password:Logpresso SNR-4.0.2409.1 (build 20241213) on Araqne Core 4.0.2logpresso@forwarder logpresso>

전달 노드 GUID 설정

아래의 명령어를 입력하여 전달 노드의 GUID를 설정합니다. 전달 노드의 GUID는 전달 노드 설정 추가 단계에서 노드 추가 후 다시 조회하면 확인할 수 있습니다.



logpresso> sonar.setGuid GUID\_문자열

암호화 키 설정

아래의 명령어를 입력하여 이전 단계에서 확인한 암호화 키를 설정합니다.

logpresso> sonar.setCipherKey 암호화\_키\_문자열

인증서 설정

최초 전달 서버 시작 시 자동 생성된 인증서를 조회하여 확인합니다.

logpresso> keystore.listKey Stores-------------[logpresso-ca] type: JKS, path: /data/logpresso-data/logpresso-ca/certs/ca.jks[logpresso-ca-key] type: PKCS12, path: /data/logpresso-data/logpresso-ca/certs/ca.pfx[logpresso-web] type: PKCS12, path: /data/logpresso-data/logpresso-ca/certs/web.pfx[logpresso-base] type: PKCS12, path: /data/logpresso-data/logpresso-ca/certs/base.pfx

자동 생성된 인증서를 모두 삭제합니다.

logpresso> keystore.unregister logpresso-calogpresso> keystore.unregister logpresso-ca-keylogpresso> keystore.unregister logpresso-weblogpresso> keystore.unregister logpresso-base

분석 서버에서 다운로드한 인증서를 기존 경로에 복사하고, 아래와 같이 다시 등록합니다. 인증서 암호는 최초 설치 시 설치 마법사에서 설정한 암호입니다.

logpresso> keystore.register logpresso-ca JKS /data/logpresso-data/logpresso-ca/certs/ca.jkslogpresso> keystore.register logpresso-base PKCS12 /data/logpresso-data/logpresso-ca/certs/base.pfxlogpresso> keystore.register logpresso-sentry PKCS12 /data/logpresso-data/logpresso-ca/certs/sentry.pfxlogpresso> keystore.register logpresso-storage PKCS12 /data/logpresso-data/logpresso-ca/certs/storage.pfxlogpresso> keystore.register logpresso-web PKCS12 /data/logpresso-data/logpresso-ca/certs/web.pfx

웹 서버 설정

전달 서버에서 현재 열려있는 웹 포트 목록을 확인합니다.

logpresso> httpd.bindings/0.0.0.0:8443 (ssl: key logpresso-web, trust null), opened, default context: webconsole, idle timeout: 0seconds, log file prefix: null, access log: false, error log: false/0.0.0.0:18443 (ssl: key logpresso-web, trust null), opened, default context: sonar-explanation, idle timeout: 0seconds, log file prefix: null, access log: false, error log: false/0.0.0.0:443 (ssl: key logpresso-web, trust null), opened, default context: sonar, idle timeout: 0seconds, log file prefix: null, access log: false, error log: false/0.0.0.0:44300 (ssl: key logpresso-web, trust null), opened, default context: deploy, idle timeout: 0seconds, log file prefix: null, access log: false, error log: false

자동으로 열린 웹 포트를 모두 닫고 인증서 변경을 반영하여 필수 포트만 다시 개방합니다.

logpresso> httpd.close 8443logpresso> httpd.close 18443logpresso> httpd.close 443logpresso> httpd.close 44300logpresso> httpd.openSsl 8443 webconsole logpresso-web

정책 동기화 설정

분석 서버에서 전달 서버에 접속할 수 있도록 웹 관리콘솔에서 노드 추가 시 설정한 암호로 전달 서버의 정책 동기화 암호를 재설정합니다.

logpresso> dom.resetPassword localhost rootNew Password:

이어서 아래의 명령어를 입력하여 정책 동기화를 설정합니다. host 항목에 입력하는 주소는 애플리케이션 로드 밸런서(ALB)의 IP 주소 또는 분석 서버에 할당된 가상 IP 주소를 입력해야 합니다.

logpresso> sonar.setMasterhost? x.x.x.xport? 443account? rootpassword? connect timeout? 10000read timeout? 10000secure? trueskip cert check? trueset

이 단계를 완료한 후 로그프레소 클라우드 또는 로그프레소 소나 웹 관리 콘솔의 클러스터 메뉴에서 전달 서버의 상태가 녹색으로 표시됨을 확인할 수 있습니다.

RPC 연결 접속

웹 관리 콘솔의 클러스터 설정 화면에서 전달 노드 추가 시 지정한 노드 ID를 이용하여 아래와 같이 고유 식별자를 설정합니다. 전달 노드 추가 화면의 예시에서는 f1에 해당됩니다.

logpresso> forwarder.setGuid [전달노드 ID]

로그프레소 클라우드인 경우 각 인스턴스의 IP 주소, 로그프레소 소나 구성인 경우 분석 서버의 IP 주소를 입력합니다. 2개의 RPC 연결을 동시에 유지해야 하므로 여기에서는 각 분석 서버의 실제 IP 주소를 입력해야 합니다.

버퍼 크기는 바이트 단위로 숫자만 입력하며, 서버 연결 단절 시 목표하는 기간 동안 데이터를 유지할 수 있도록 충분한 크기를 지정합니다.

logpresso> forwarder.addBase control\_1 [분석서버A IP주소] 7140 logpresso-sentry logpresso-ca [버퍼 크기]logpresso> forwarder.addBase control\_2 [분석서버B IP주소] 7140 logpresso-sentry logpresso-ca [버퍼 크기]

분석 노드가 단일 서버로 구성된 경우에는 분석서버B 추가 단계를 건너뜁니다.

로그프레소 분석 노드 쌍을 지정합니다. 아래의 명령어는 control\_1과 control\_2를 control이라는 이름의 단일 고가용성 구성 단위로 지정합니다.

logpresso> forwarder.addBasePair control control\_1 control\_2

분석 노드가 단일 서버로 구성된 경우에는 control\_2를 control\_1로 입력합니다.

시스템 로그 전송 설정

전달 노드의 시스템 로그를 분석 서버에 전송하도록 설정합니다. 네트워크 로드 밸런서의 IP 주소 또는 분석 서버의 가상 IP 주소를 지정합니다.

logpresso> sentry.setGuid [전달노드 ID]oklogpresso> sentry.addBase control [NLB IP] 7140 logpresso-sentry logpresso-ca 10485760000base added

#### 설치 검증

접속 상태 확인

웹 관리 콘솔의 클러스터 메뉴에서 새로 추가한 전달 노드의 접속 상태가 녹색으로 표시되면 정상적으로 구성이 완료된 것입니다. 만약 접속 상태가 회색에서 변경되지 않는 경우에는 [연결 문제 진단](https://docs.logpresso.com/ko/sonar/4.0/forwarder/ko/sonar/4.0/forwarder/troubleshoot-connection) 절을 참고하여 문제를 해결하세요.

앱 재설치

전달 서버를 설치하기 전에 웹 관리 콘솔에서 설치한 앱은 자동으로 설치되지 않으므로, 필요 시 앱 재설치를 통해 전달 서버에 앱을 설치해야 합니다.

### 업그레이드

#### 사전 점검

로그프레소 분석 서버 및 수집 서버는 하위 호환성을 유지하도록 설계되어 있습니다. 즉, 릴리스 노트에 특별히 전달 서버 업그레이드 요구사항이 없다면 로그프레소 클라우드 인스턴스 또는 로그프레소 소나 클러스터가 업그레이드 되어도 전달 서버는 무중단으로 운영을 지속할 수 있습니다.

전달 서버를 업그레이드하는 경우, 분석 서버와 수집 서버는 전달 서버보다 높은 버전으로 이미 업그레이드된 상태여야 합니다.

#### 수행 절차

새 로그프레소 소나 패키지를 /opt/logpresso 디렉터리에 업로드합니다.

패키지 파일의 소유권을 logpresso 계정으로 변경합니다.

$ sudo chown logpresso:logpresso /opt/logpresso/logpresso-SNR-4.0.XXXX.0-uNNNN.zip

logpresso 계정으로 전환합니다.

$ sudo su - logpresso

Logpresso 설치 디렉토리로 이동합니다.

$ cd /opt/logpresso

기존 캐시 디렉토리를 백업합니다.

$ mkdir backup; tar czf cache-$(date +%Y%m%d).tar.gz cache/; mv cache-$(date +%Y%m%d).tar.gz backup/

기존 confdb 디렉토리를 백업합니다.

$ tar czf confdb-$(date +%Y%m%d).tar.gz data/araqne-confdb/; mv confdb-$(date +%Y%m%d).tar.gz backup/

Logpresso 데몬을 중지합니다.

$ sudo systemctl stop logpresso

캐시 디렉토리를 삭제합니다. 기존 디렉터리를 삭제하지 않고 덮어쓰면 번들 종속성 오류로 인해 정상적으로 부팅되지 않으므로 유의합니다.

$ rm -rf cache

새 Logpresso 패키지를 압축 해제합니다.

$ unzip logpresso-SNR-4.0.XXXX.0-uNNNN.zip

Logpresso 데몬을 시작합니다.

$ sudo systemctl start logpresso

Logpresso 데몬이 부팅된 후 /opt/logpresso/log/araqne.log 파일에 오류 로그가 없고 로그가 정상적으로 수집 및 저장되는지 확인합니다.

### 데몬 시작

아래 명령어를 입력하여 로그프레소 전달 서버 데몬을 시작할 수 있습니다.

$ sudo systemctl start logpresso

아래 명령어를 사용하면 최근 systemd 로그를 조회할 수 있습니다.

$ sudo journalctl -xe

로그프레소 전달 서버 데몬과 관련된 systemd 로그만 조회하려면 아래와 같이 필터링합니다. 로그 조회를 종료하려면 q키를 입력합니다.

$ sudo journalctl -xe -u logpresso.serviceJan 30 05:47:47 HOSTNAME logpresso[18408]: Logpresso Launcher 1.1.0Jan 30 05:47:47 HOSTNAME logpresso[18408]: starting Logpresso...Jan 30 05:47:48 HOSTNAME logpresso[18408]: Logpresso CLI is now listening on 7022 as SSH.Jan 30 05:47:48 HOSTNAME logpresso[18408]: Logpresso has been started.Jan 30 05:47:49 HOSTNAME systemd[1]: Started Logpresso daemon.

### 데몬 종료

아래 명령어를 입력하여 로그프레소 전달 서버 데몬을 종료할 수 있습니다.

$ sudo systemctl stop logpresso

종료 진행 상태를 확인하려면 아래와 같이 systemd 로그를 조회합니다. 로그 조회를 종료하려면 q키를 입력합니다.

$ sudo journalctl -xe -u logpresso.serviceJan 30 09:13:24 HOSTNAME logpresso[70620]: stopping Logpresso. waiting for shutdown ................ stoppedJan 30 09:13:25 HOSTNAME systemd[1]: logpresso.service: Deactivated successfully.Jan 30 09:13:25 HOSTNAME systemd[1]: Stopped Logpresso daemon.

### 데몬 상태 조회

전달 서버의 리눅스 셸에서 아래와 같이 로그프레소 전달 서버의 서비스 상태를 조회할 수 있습니다. 상태 조회를 종료하려면 q키를 입력합니다.

$ sudo systemctl status logpresso● logpresso.service - Logpresso daemon Loaded: loaded (/usr/lib/systemd/system/logpresso.service; disabled; preset: disabled) Active: active (running) since Thu 2025-01-30 09:16:03 UTC; 1s ago Docs: https://ko.logpresso.com/documents Process: 70687 ExecStart=/opt/logpresso/logpresso start (code=exited, status=0/SUCCESS) Main PID: 70726 (java) Tasks: 44 (limit: 47391) Memory: 647.7M CPU: 10.422s CGroup: /system.slice/logpresso.service └─70726 /opt/logpresso/jdk-11.0.14.1-jemalloc/bin/java -Xms4G -Xmx4G -XX:MaxDirectMemorySize=1G -XX:-OmitStackTraceInFastThrow -XX:-UseCompressed>Jan 30 09:16:00 HOSTNAME systemd[1]: Starting Logpresso daemon...Jan 30 09:16:01 HOSTNAME logpresso[70687]: Logpresso Launcher 1.1.0Jan 30 09:16:01 HOSTNAME logpresso[70687]: starting Logpresso...Jan 30 09:16:03 HOSTNAME logpresso[70687]: Logpresso CLI is now listening on 7022 as SSH.Jan 30 09:16:03 HOSTNAME logpresso[70687]: Logpresso has been started.Jan 30 09:16:03 HOSTNAME systemd[1]: Started Logpresso daemon.

### 수집 설정

모든 수집 설정은 로그프레소 클라우드 또는 로그프레소 소나의 웹 관리 콘솔에서 관리할 수 있습니다.

웹 관리 콘솔에서 수집기를 추가할 때 수집 위치를 새로 추가한 전달 노드로 지정하면 전달 노드를 통해 데이터를 수집할 수 있습니다. UI 매뉴얼의 [수집기 공통 설정](https://docs.logpresso.com/ko/sonar/4.0/forwarder/ko/sonar/4.0/ui/section-loggers) 항목을 참조하세요.

## 트러블슈팅

### 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

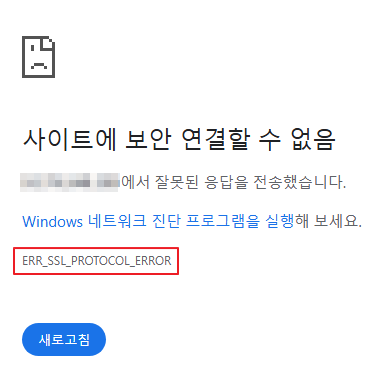
tcpscan 명령 시 일정 시간 후에 timeout이 표시된다면 분석 서버에서 전달 서버에 이르는 통신 경로에 위치한 모든 방화벽의 정책을 재확인합니다.

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)

### Syslog 수신 진단

웹 관리 콘솔에서 수집기를 설정해도 전달 서버를 경유하여 Syslog가 정상적으로 수집되지 않는 경우에는 아래와 같이 진단합니다. 아래 예시에서는 IP 주소 172.20.100.100에서 패킷을 전송한다고 가정합니다.

#### 전달 서버 트레이스

리눅스 셸에서 아래 명령어로 로그프레소 셸에 진입합니다.

$ ssh -p7022 root@localhost

Syslog 서버 설정 목록을 조회합니다.

logpresso> syslog.serversSyslog Servers----------------[logpresso] 0.0.0.0:514 (udp), charset=UTF-8 (override: 0), capacity=20000, rx\_buf\_size=0, receiver\_cpu\_id=-1, queue\_count=1, buffer\_file\_path=./, buffer\_file\_size=10737418240, start from=2024-12-11 13:22:13, received=7

아래와 같이 클라이언트 IP 주소별 수신 통계를 조회할 수 있습니다.

logpresso> syslog.stats logpressoSyslog Statistics-------------------x.x.x.x => 1 (first seen 2025-01-20 10:58:44, last seen 2025-01-20 10:58:44)

아래와 같이 실시간으로 수신되는 Syslog 패킷 내용을 추적할 수 있습니다. Ctrl+C 키 조합으로 중단합니다.

logpresso> syslog.trace logpressopress ctrl-c to stop------------------------

#### Syslog 패킷 확인

tcpdump 명령어를 이용하여 패킷이 로그프레소 전달 서버에 도달하는지 검증합니다.

# tcpdump -i any host 172.20.100.100 port 514 -A

#### 포트 개방 확인

전달 서버에 Syslog 패킷이 도달하고 있는 것이 확인되었다면 포트가 열려있는지 확인합니다.

# netstat -na | grep :514udp 0 0 0.0.0.0:514 0.0.0.0:\*

위와 같이 포트가 열려있지 않다면 설치 단계에서 [JVM 권한 부여 단계](https://docs.logpresso.com/ko/sonar/4.0/forwarder/ko/sonar/4.0/forwarder/deploy-forwarder)를 누락하여 포트 개방에 실패했거나, 포트 설정이 변경되었을 수 있습니다.

아래 명령어를 실행하여 cap\_net\_raw가 출력되는지 확인합니다.

# getcap /opt/logpresso/java/jdk-11.0.14.1-jemalloc/bin/java

권한이 부여되어 있지 않다면 setcap 단계를 다시 수행하고 데몬을 재시작합니다.

#### 호스트 방화벽 정책 확인

Syslog 패킷이 수신되고 514 포트가 열려있는데 로그가 수신되지 않는다면 호스트 방화벽 정책을 다시 확인합니다.

# firewall-cmd --list-ports

#### rp\_filter 설정 확인

방화벽 정책, 포트 개방 상태가 모두 정상인데 로그프레소 셸에서 syslog.trace 명령으로 수신을 확인할 수 없는 경우에는 Reverse Path Filtering 문제일 수 있습니다.

리눅스 커널의 [Reverse Path Filtering](https://tldp.org/HOWTO/Adv-Routing-HOWTO/lartc.kernel.rpf.html) 기능은 패킷의 출처를 확인하여 스푸핑된 패킷을 차단하는 기능입니다. 기본값은 1로 설정되어 있으며 유효하지 않은 경로에서 들어오는 패킷을 버립니다.

즉, 전달 서버에 여러 개의 네트워크 인터페이스 카드가 구성된 경우에 발생할 수 있는 문제이며, 아래와 같이 설정을 변경한 후 패킷이 정상적으로 수신되는지 다시 확인합니다.

**기존 설정 확인**

예를 들어 eth2 인터페이스라면 아래와 같이 명령어를 입력합니다.

# cat /proc/sys/net/ipv4/conf/eth2/rp\_filter1

/etc/sysctl.conf 파일 끝에 아래 설정을 추가합니다.

net.ipv4.conf.eth2.rp\_filter = 2

관리자 권한으로 아래 명령어를 실행하여 커널 설정을 변경합니다.

# sysctl -p

**rp\_filter 설정 값**

* 0 (비활성화): Reverse Path Filtering을 수행하지 않음
* 1 (기본값, 엄격): 패킷의 출발지 IP 주소를 기준으로 해당 인터페이스의 경로를 확인하고, 일치하지 않으면 패킷을 드롭
* 2 (느슨함): 동일한 출발지 IP 주소를 가진 패킷이 어느 인터페이스를 통해서든 유효한 경로를 가지면 허용