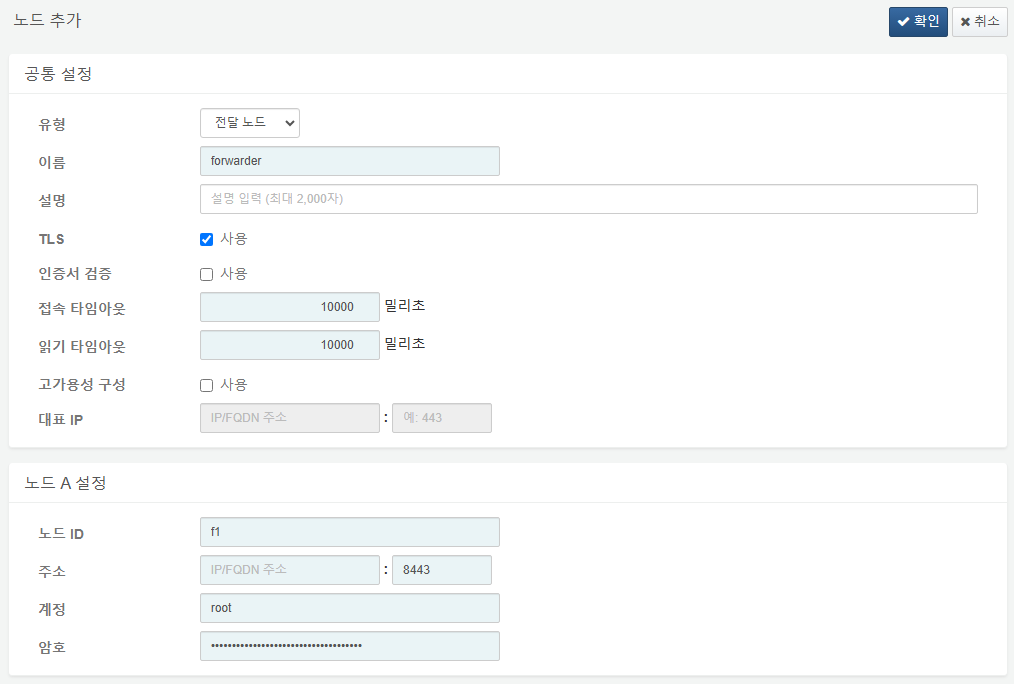
### 설치

#### 분석 서버 작업

전달 노드 설정 추가

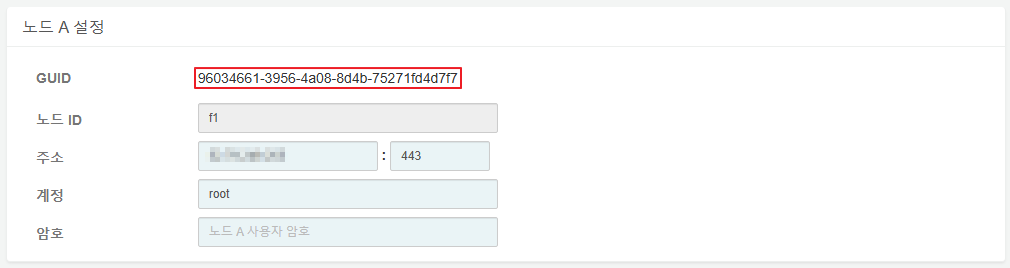
로그프레소 클라우드 또는 로그프레소 소나의 웹 관리 콘솔에서 아래와 같이 전달 노드 설정을 추가합니다.



* 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

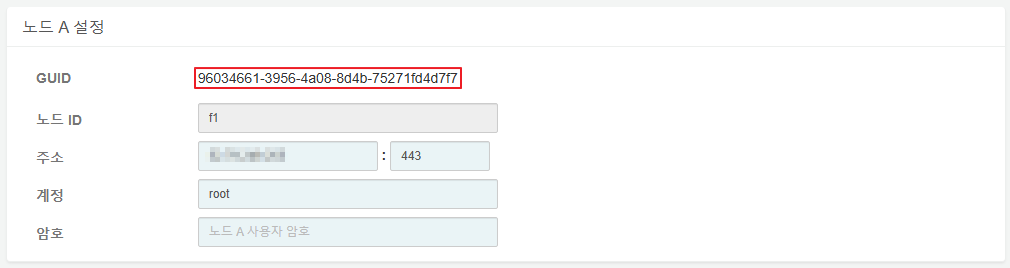
#### 접속 설정

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.