### 센트리

#### 개요

센트리는 로그프레소 플랫폼의 로그 수집 에이전트입니다. 센트리와 로그프레소 서버는 인증서 기반 상호 인증을 거친 후 TLS 채널을 통해 안전하게 로그를 전송합니다.

로그프레소 4.0.2312.0 버전에서 센트리 관리 기능의 편의성을 개선했습니다. 명령어 한 줄로 간편하게 센트리를 설치할 수 있습니다. 개선된 센트리 관리 기능은 다음과 같은 네트워크 포트를 이용합니다.

* TCP 7140: 센트리와 로그프레소 서버 간 데이터 통신
* TCP 44300: 센트리 설치 파일 및 센트리 인증서 배포

로그프레소 서버가 센트리로부터 데이터를 수신할 수 있도록 서버의 로컬 방화벽에서 해당 포트를 개방해야 합니다. 포트는 운영 환경에 따라 변경될 수 있습니다.

#### 배포 준비

센트리를 배포하려면 JDK와 센트리 설치용 패키지가 필요합니다.

JAVA

센트리를 실행하려면 JAVA(JRE 또는 JDK)가 필요합니다. 센트리를 실행하는데 필요한 자바는 로그프레소 서버에서 센트리 설치 파일과 함께 배포합니다.

JRE/JDK 준비

먼저 신뢰할 수 있는 JRE 또는 JDK를 준비하세요. [Adoptium](https://adoptium.net/temurin/releases), [마이크로소프트](https://learn.microsoft.com/ko-kr/java/openjdk/download) 등 신뢰할 수 있는 OpenJDK 사이트에서 JRE 또는 JDK를 다운로드하세요. 다운로드할 JRE/JDK는 확장자가 **.tar.gz**(리눅스용)이거나, **.zip**(윈도우용)이어야 합니다.

다운로드한 파일을 로그프레소 서버에 업로드하기 전에 파일 이름을 다음 규칙에 맞도록 변경하세요.

* 파일 이름은 jdk- 또는 jre-로 시작해야 합니다.
* jdk- 또는 jre- 뒤부터 가장 처음 오는 점(.) 사이에 숫자만으로 구성된 메이저 버전이 표기되어야 합니다.
* 로그프레소 서버가 식별할 수 있는 파일명(예)
* jre-**\_11\_**.0.14.1.tar.gz (버전을 11.0.14로 상세히 표기)
* jdk-**\_11\_**.zip (버전을 11로 약식 표기)
* 로그프레소 서버가 식별하지 못하는 파일명(예)
* jre-**\_8u151-linux-x64\_**.tar.gz (버전 표기에 숫자 외에 문자열이 포함되어 있음)
* 리눅스용 JRE/JDK 파일 확장자는 tar.gz이어야 합니다.
* 윈도우용 JRE/JDK 파일 확장자는 zip이어야 합니다.

JRE/JDK 업로드

다음 명령을 참고해 로그프레소 서버에서 JRE/JDK 파일을 배포용 디렉터리에 옮겨놓으세요.

# 이용 환경에 맞게 수정해 사용하세요.# PKGDIR: 로그프레소 서버 파일이 있는 디렉터리PKGDIR="/opt/logpresso"# 리눅스용/윈도우용 JRE 디렉터리 생성sudo -u logpresso mkdir -p ${PKGDIR}/download/{linux,win}/x64# 설치 파일 복사sudo -u logpresso cp PATH\_TO\_JRE\_TAR\_GZ {PKGDIR}/linux/x64sudo -u logpresso cp PATH\_TO\_JRE\_ZIP {PKGDIR}/win/x64

센트리 설치용 패키지

**시스템 > 패키지 관리**에 센트리 설치에 사용할 패키지를 등록해야 합니다. 패키지를 등록하는 방법은 [패키지 관리](https://docs.logpresso.comnull)를 참고하세요.

로그프레소 서버로 배포할 수 있는 센트리는 버전 2312.0 및 이후 버전입니다. 이전 버전은 수동 배포만 지원합니다.

#### 센트리 설치

관리대상 서버에 센트리를 설치하는 과정은 크게 두 단계로 나뉩니다.

* 센트리 추가
* 관리대상 서버에서 센트리 설치 명령 실행

센트리 설치 명령은 설치할 센트리의 식별자와 센트리가 접속할 서버 정보, 설치 시 인증서 발급 및 호스트 인증에 사용할 인증 토큰 정보로 구성됩니다. 설치 명령은 센트리를 설치할 호스트의 운영체제가 리눅스인 경우, 배시 셸을 기준으로, 윈도우인 경우 파워셸을 기준으로 생성됩니다. 생성된 명령을 해당 호스트에서 실행하면 센트리와 JRE의 설치와 서버로 연결이 모두 자동으로 수행됩니다.

1 단계: 센트리 추가

센트리를 추가하는 방법은 다음과 같습니다.

**시스템 > 센트리**에서 도구 모음에 있는 **추가**를 클릭하세요.

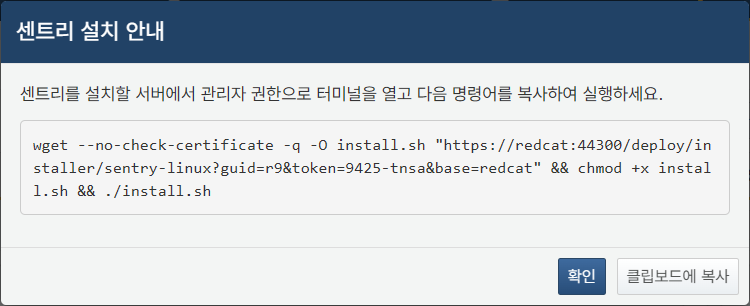


**센트리 추가** 대화상자에서 센트리를 설치에 필요한 정보를 입력하고 **추가**를 클릭하세요.



* **운영체제**: 센트리를 설치할 호스트의 운영체제(**리눅스**, **윈도우** 중에서 선택)
* **센트리 ID**: 센트리를 식별할 고유 ID
* **접속 대상**: 센트리가 접속할 서버를 목록에서 선택하세요. **시스템 > 클러스터 노드**에 등록된 클러스터 노드의 목록이 표시됩니다.
* **인증 토큰**: 무작위로 부여되는 센트리 설치용 인증 토큰(예: 9425-tnsa)

**센트리 설치 안내** 메시지의 안내에 따라 설치 명령을 복사한 다음, 센트리를 설치할 호스트의 관리자 터미널에서 실행하세요.



* **클립보드 복사**를 클릭하면 사용자 PC의 클립보드에 설치 명령이 복사됩니다.
* **확인**을 클릭하면 창이 닫힙니다.

리눅스

리눅스용 설치 명령은 배시셸에서 실행됩니다. 설치 명령은 다음과 같은 형식으로 되어 있습니다. 대문자로 표기된 부분은 설치 명령이 생성될 때 자동으로 부여됩니다.

# ADDR\_1: 센트리 패키지 및 인증서를 배포하는 서버 주소# GUID: 센트리 ID# TOKEN: 인증 토큰# ADDR\_2: 센트리와 통신할 서버의 주소(접속 대상)wget --no-check-certificate -q -O install.sh \"https://ADDR\_1:44300/deploy/installer/sentry-linux?guid=GUID&token=TOKEN&base=ADDR\_2" && \chmod +x install.sh && \./install.sh

리눅스에 wget이 없고 대신에 curl만 있으면 설치 명령을 다음과 같이 수정해서 사용하세요.

# ADDR\_1: 센트리 패키지 및 인증서를 배포하는 서버 주소# GUID: 센트리 ID# TOKEN: 인증 토큰# ADDR\_2: 센트리와 통신할 서버의 주소(접속 대상)curl -k -s -o install.sh \"https://ADDR\_1:44300/deploy/installer/sentry-linux?guid=GUID&token=TOKEN&base=ADDR\_2" && \sed -i 's/wget --no-check-certificate -q -O/curl -k -s -o/g' install.sh && \chmod +x install.sh && \./install.sh

윈도우

설치 명령은 다음과 같은 형식으로 되어 있습니다. 대문자로 표기된 부분은 설치 명령이 생성될 때 자동으로 부여됩니다.

# ADDR\_1: 센트리 패키지 및 인증서를 배포하는 서버 주소# GUID: 센트리 ID# TOKEN: 인증 토큰# ADDR\_2: 센트리와 통신할 서버의 주소(접속 대상)cd $env:TEMP;add-type " using System.Net; using System.Security.Cryptography.X509Certificates; public class TrustAllCertsPolicy : ICertificatePolicy { public bool CheckValidationResult(ServicePoint a, X509Certificate b, WebRequest c, int d) { return true; } }";[System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicyInvoke-WebRequest `-Uri 'https://ADDR\_1:44300/deploy/installer/sentry-linux?guid=GUID&token=TOKEN&base=ADDR\_2' `-OutFile install.cmd; cmd /c install.cmd

로그프레소 서버가 제공하는 설치 명령은 모든 윈도우에 기본 탑재되는 파워셸 5.1을 기준으로 합니다. 사용하는 파워셸이 버전 5.1 또는 이후 버전인 경우 다음과 같이 수정해서 실행하세요.

# ADDR\_1: 센트리 패키지 및 인증서를 배포하는 서버 주소# GUID: 센트리 ID# TOKEN: 인증 토큰# ADDR\_2: 센트리와 통신할 서버의 주소(접속 대상)Set-Location $env:TEMP;Invoke-WebRequest -SkipCertificateCheck `-Uri 'https://ADDR\_1:44300/deploy/installer/sentry-linux?guid=GUID&token=TOKEN&base=ADDR\_2' `-OutFile install.cmd; cmd /c install.cmd

명령행을 실행할 수 있는 파워셸 버전은 윈도우에서 기본 제공하는 버전인 5.1입니다. Windows Terminal에서 파워셸 버전 5.1은 "Windows PowerShell"로, 그 이후 버전은 "PowerShell"로 표기되므로 파워셸을 실행할 때 확인하세요.

2 단계: 센트리 설치

클립보드에 복사한 내용을 센트리를 설치할 호스트에서 실행하면 센트리가 설치되고, 자동으로 실행됩니다.

리눅스 센트리가 설치되는 디렉터리는 /opt/logpresso-sentry, 윈도우 센트리 설치 디렉터리는 C:\Program Files\Logpresso Sentry입니다.

리눅스

리눅스 환경에서 센트리의 설치하고 실행하려면 **net-tools**, **unzip**, **wget**이 설치되어 있어야 합니다. 설치되어 있지 않다면 다음 명령을 실행해서 설치해주세요.

# unzip, wget은 센트리를 설치할 때 필요합니다. # net-tools는 센트리가 시스템 정보를 수집할 때 필요합니다. # RHEL 계열 sudo dnf install net-tools unzip wget # Debian 계열 sudo apt-get install net-tools unzip wget

배시 셸(Bash)에서 **[1 단계: 센트리 설치 명령 생성](section-sentries#outline9)** 에서 생성한 명령행을 **root** 권한으로 실행하세요.

로그프레소 서버에서 다음 명령으로 센트리의 상태를 확인하세요.

systemctl status logpresso-sentry.service

로그프레소 서버에서 [센트리의 연결 상태를 확인](https://docs.logpresso.comnull)하세요. 센트리의 연결 상태가 녹색으로 표시되지 않으면 센트리와 서버의 로컬 방화벽과 네트워크 통신 구간을 점검해보세요.

윈도우

관리자 권한으로 파워셸을 열고 **[1 단계: 센트리 설치 명령 생성](section-sentries#outline9)** 에서 생성한 명령행을 실행하세요.

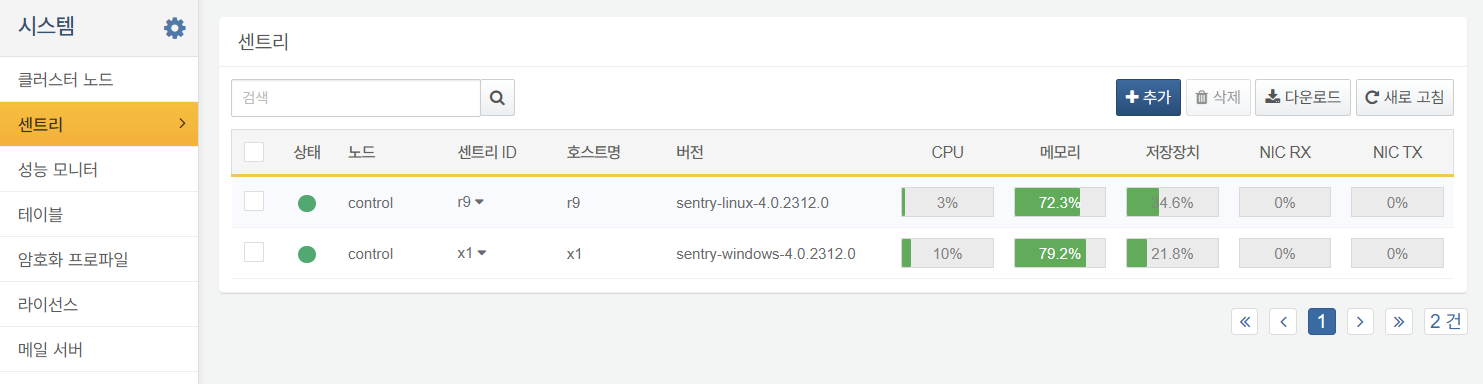
**작업 관리자**의 **서비스** 탭에서 **Logpresso** 서비스가 **실행 중**으로 표시되는지 확인하세요. 파워셸에서 확인하려면 다음 명령을 실행하세요.

sc.exe query Logpresso

로그프레소 서버에서 [센트리의 연결 상태를 확인](https://docs.logpresso.comnull)하세요. 센트리의 연결 상태가 녹색으로 표시되지 않으면 센트리와 서버의 로컬 방화벽과 네트워크 통신 구간을 점검해보세요.

#### 센트리 상태 조회

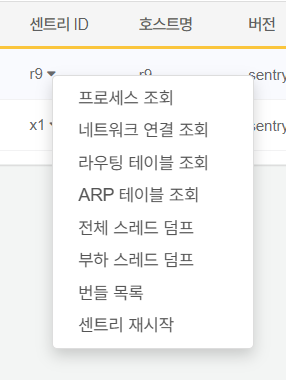
센트리 목록에서 센트리의 상태를 확인할 수 있습니다.

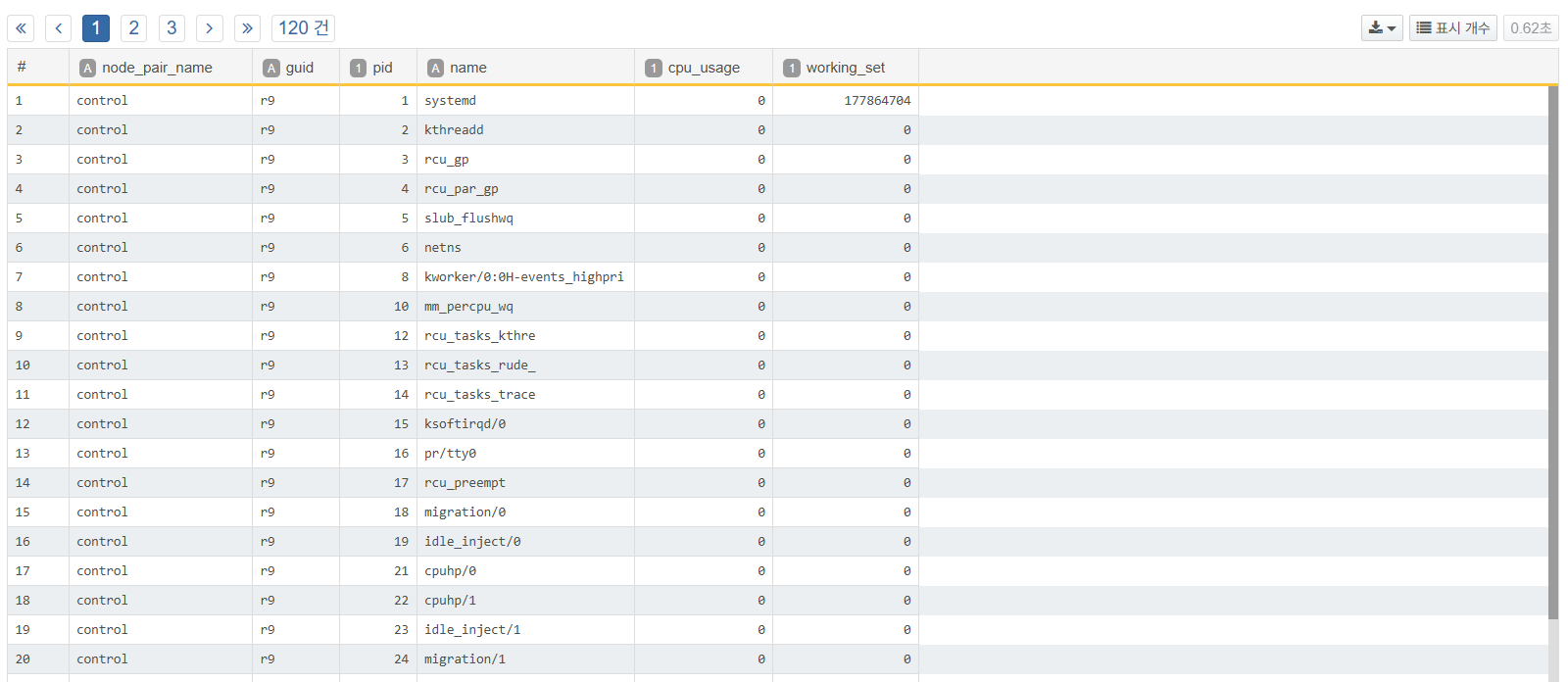
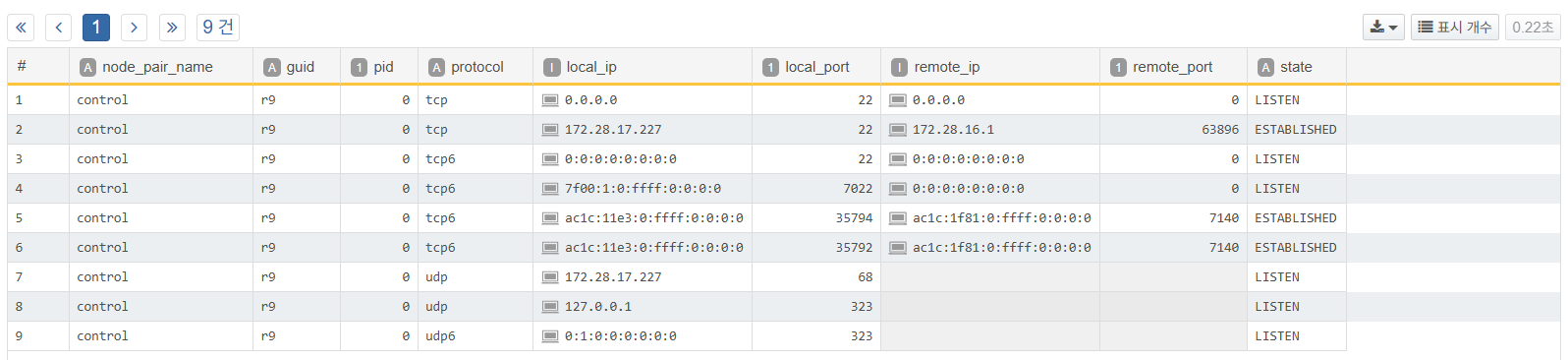
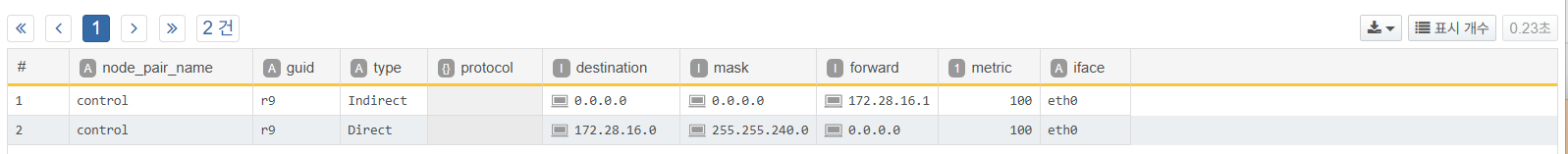
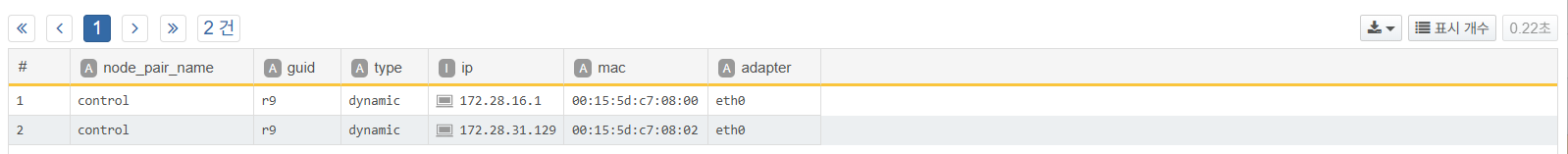
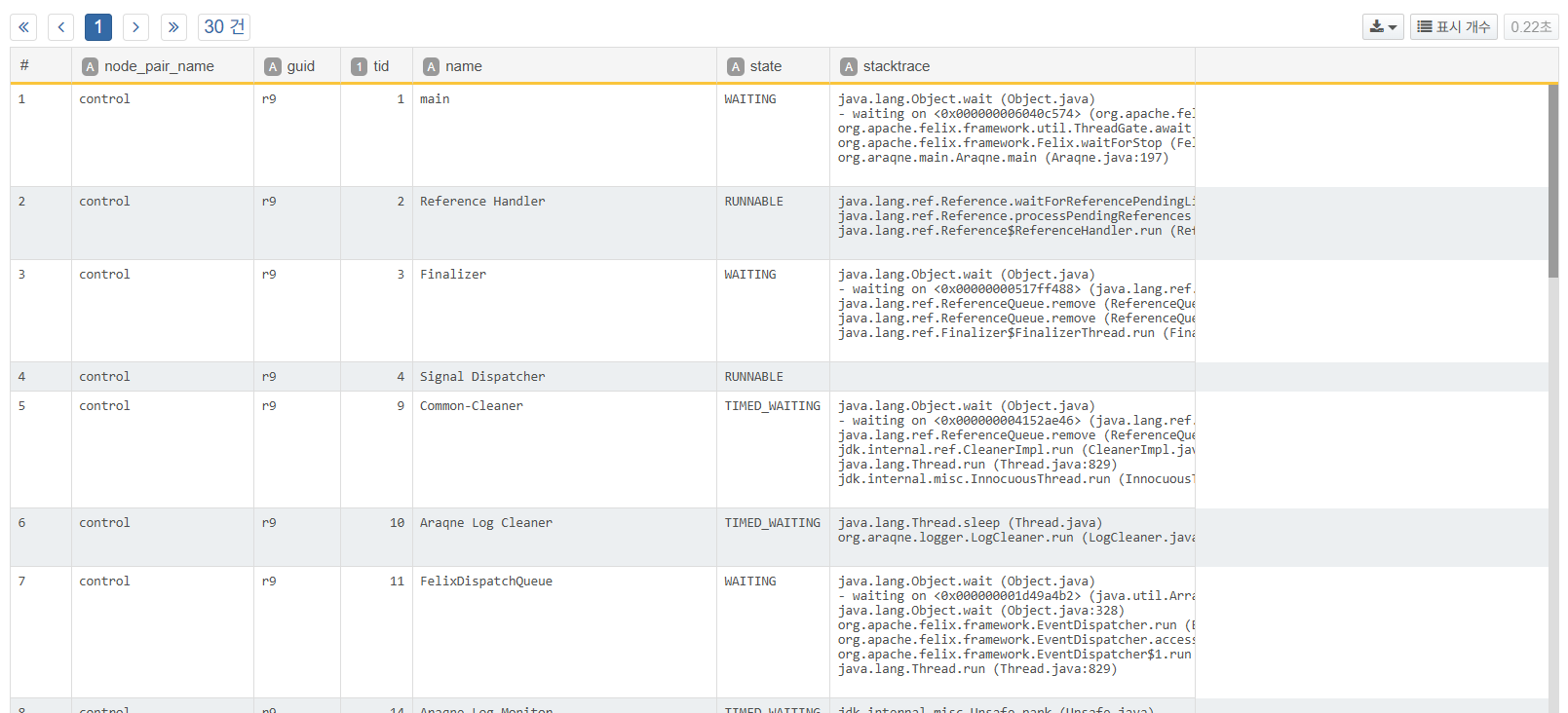
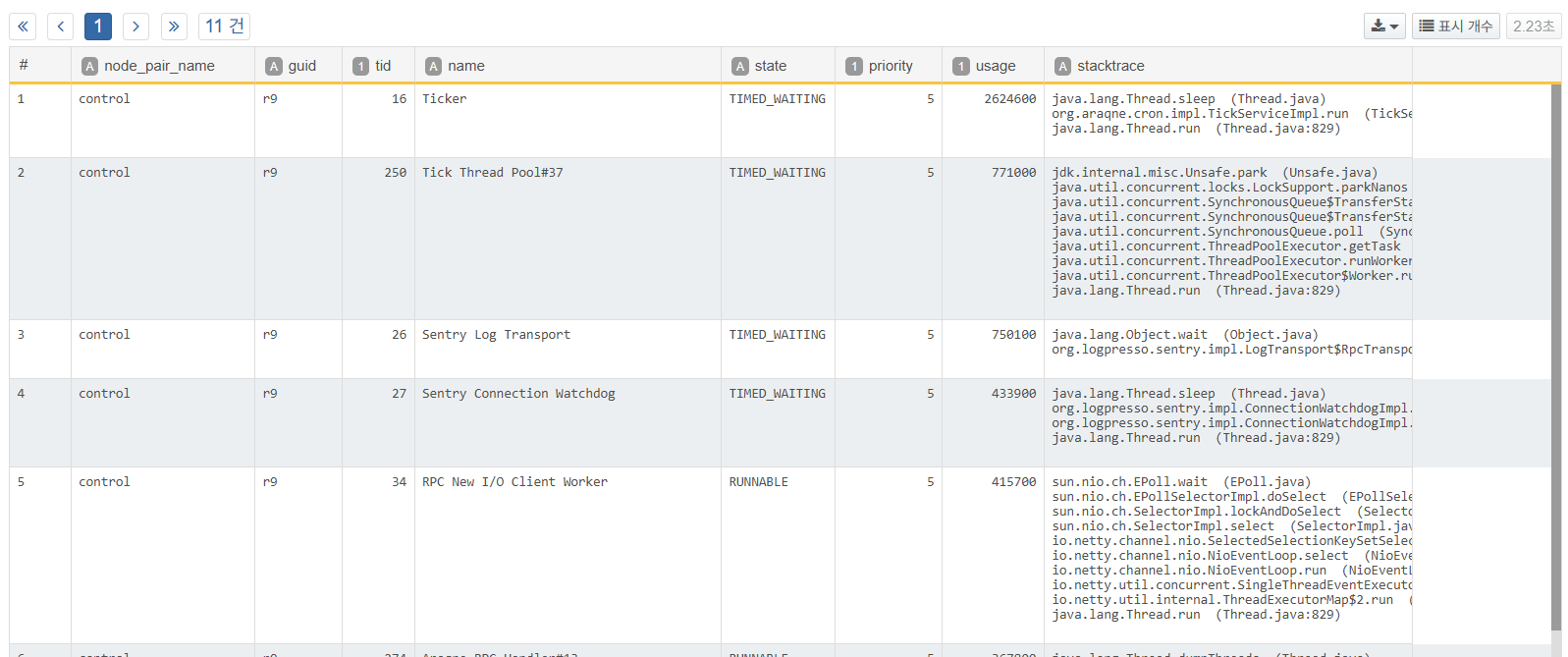
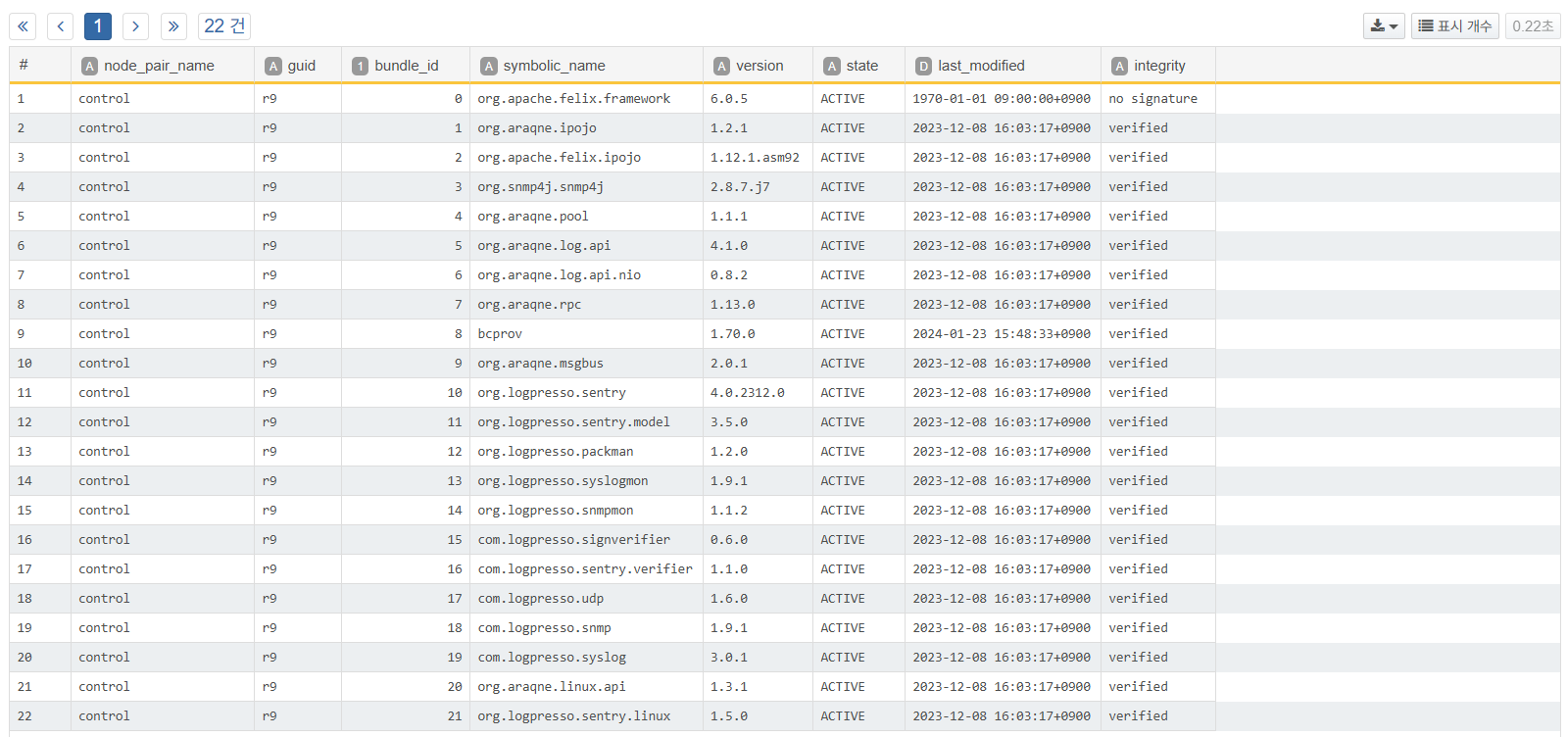


* **상태**: 센트리가 서버와 연결되면 녹색, 센트리가 연결되지 않으면 회색으로 표시합니다.
* **노드**: 센트리를 제어하는 클러스터 노드의 이름을 보여줍니다.
* **센트리 ID**: 센트리 추가 시 입력한 센트리 ID
* **호스트명**: 센트리가 설치된 호스트의 이름
* **버전**: 설치된 센트리의 버전 정보
* **CPU**: CPU 사용량(단위: 백분율)
* **MEM**: 메모리 사용량(단위: 백분율)
* **DISK**: 스토리지 사용량(단위: 백분율). 저장장치 파티션이 여러 개인 경우 최댓값을 표시
* **NIC RX**: 네트워크 수신 대역폭 사용량(단위: 백분율). 네트워크 인터페이스가 여러 개인 경우 최댓값을 표시
* **NIC TX**: 네트워크 전송 대역폭 사용량(단위: 백분율). 네트워크 인터페이스가 여러 개인 경우 최댓값을 표시

#### 센트리 원격 관리

센트리 ID를 클릭하면 센트리 호스트의 프로세스 목록 조회, 네트워크 연결 정보, 라우팅 테이블, ARP 캐시, 스레드 덤프, 번들 목록 조회 및 무결성 검사, 센트리 재시작 등과 같은 센트리 관리 기능을 수행할 수 있습니다.



* **프로세스 목록**: 센트리 호스트의 프로세스 목록을 보여줍니다.
* **네트워크 연결**: 센트리 호스트가 연결하거나 연결된 네트워크 세션 목록을 보여줍니다.
* **라우팅 테이블**: 센트리 호스트의 라우팅 테이블을 보여줍니다.
* **ARP 캐시 테이블**: 센트리 호스트에 캐시된 ARP 정보를 보여줍니다.
* **전체 스레드 덤프**: 센트리가 실행되는 동안 사용하는 스레드 목록을 보여줍니다.
* **부하 스레드 덤프**: 스레드의 시스템 부하를 확인할 수 있습니다.
* **번들 목록**: 센트리에 설치된 번들 목록을 보여줍니다.
* **에이전트 재시작**: 센트리를 재시작합니다.

#### 센트리 삭제

센트리를 완전히 삭제하려면 먼저 관리대상 호스트에서 센트리를 제거한 후, 로그프레소 서버에 등록된 센트리 정보를 삭제하세요.

1 단계: 센트리 삭제 명령 실행

리눅스

리눅스 호스트에서 센트리를 삭제하려면 **root** 권한으로 배시 셸(Bash)을 열고 다음 명령을 실행하세요.

# 센트리 서비스 중지sudo systemctl stop logpresso-sentry.service && \sudo /opt/logpresso-sentry/logpresso uninstall sentry && \sudo rmdir /opt/logpresso-sentry

윈도우

윈도우 호스트에서 센트리를 삭제하려면 관리자 권한으로 파워셸을 열고 다음 명령을 실행하세요.

# Logpresso 서비스 중지sc.exe stop Logpresso# Logpresso 서비스 상태 확인sc.exe query Logpresso# Logpresso 서비스 제거sc.exe delete Logpresso# 레지스트리 키 제거$reg="HKLM:\\SOFTWARE\\WOW6432Node\\Apache Software Foundation\\Procrun 2.0\\Logpresso\\"Remove-Item -Path $reg -Recurse# 센트리 파일 및 폴더 제거Set-Location "C:\Program Files\Logpresso Sentry\"# 다음 행을 실행한 후, 질문에 y로 답하세요.cmd.exe /c logpresso.cmd uninstall sentrySet-Location ..Remove-Item -Recurse -Path "C:\Program Files\Logpresso Sentry"

2 단계: 서버에서 센트리 삭제

로그프레소 서버에 등록된 센트리 정보를 삭제하는 방법은 다음과 같습니다.

**시스템 > 센트리**에서 삭제할 센트리의 체크 박스를 클릭하세요.

도구 모음에서 **삭제**를 클릭하세요.

**센트리 삭제** 대화 상자에서 **확인**을 클릭하면 선택한 센트리가 삭제됩니다. 삭제하지 않으려면 **취소**를 클릭하세요.

