### セントリー

#### 概要

セントリーは、ログプレッソ・ソナー プラットフォーム内のログ収集エージェントであり、TLSチャネルを通じてログプレッソサーバーへのログの安全な転送を保証します。このプロセスでは、相互証明書認証を用いてセキュリティを強化しています。

ログプレッソ バージョン4.0.2312.0では、セントリー管理機能が強化され、単一コマンドによるセントリーインスタンスの簡易インストールが可能となりました。強化されたセントリー管理では、以下のネットワークポートを使用します。

* TCP 7140: セントリーとログプレッソサーバー間のデータ通信
* TCP 44300: セントリーインストールファイルおよび証明書の配布

これらのポートがローカルファイアウォールで開放されていることを確認し、ログプレッソサーバーがセントリーからデータを受信できるようにしてください。なお、使用するオペレーティングシステムによっては、ポート番号が異なる場合があります。

#### セントリーのデプロイ

セントリーをデプロイするには、JDKおよびセントリーインストールパッケージが必要です。

JAVA

セントリーを実行するには、Javaランタイム環境（JRE）が必要です。JREはログプレッソサーバーから配布されるセントリーインストールファイルに同梱されています。

JREのダウンロード

まず、信頼できるJREパッケージを入手します。[Adoptium](https://adoptium.net/temurin/releases) や [Microsoft](https://learn.microsoft.com/ja-jp/java/openjdk/download) などの信頼できるOpenJDKサイトからJREファイルをダウンロードしてください。OpenJDKファイルの拡張子は、Linuxの場合は **.tar.gz**、Windowsの場合は **.zip** である必要があります。

JREファイルをログプレッソサーバーにアップロードする前に、ファイル名が以下の命名規則に従っていることを確認してください。

* ファイル名は jdk- または jre- で始まる必要があります。
* プレフィックスと最初のドット（.）の間には、数値のみのメジャーバージョン番号が入ります。
* ログプレッソサーバーで認識可能なファイル名（推奨例）:
* jre-**\_11\_**.0.14.1.tar.gz（詳細バージョン番号: 11.0.14）
* jdk-**\_11\_**.zip（簡易バージョン番号: 11）
* ログプレッソサーバーで認識できないファイル名:
* jre-**\_8u151-linux-x64\_**.tar.gz（最初のドット前に数値以外の文字が含まれている）
* Linuxの場合、JREファイルの拡張子は **tar.gz** である必要があります。
* Windowsの場合、JREファイルの拡張子は **zip** である必要があります。

JREのアップロード

JREファイルをデプロイディレクトリに移動するには、以下のコマンドを使用します。

# 環境に合わせて編集してください。# PKGDIR: ログプレッソサーバーファイルが格納されているディレクトリPKGDIR="/opt/logpresso"# Linux/Windows用のJREディレクトリを作成sudo -u logpresso mkdir -p ${PKGDIR}/download/{linux,win}/x64# インストールファイルのコピーsudo -u logpresso cp PATH\_TO\_JRE\_FILE {PKGDIR}/linux/x64sudo -u logpresso cp PATH\_TO\_JRE\_FILE {PKGDIR}/win/x64

セントリーインストールパッケージ

**設定 > パッケージ** に移動し、セントリーインストールパッケージをアップロードします。パッケージのアップロード方法については [パッケージ](https://docs.logpresso.comnull) を参照してください。

ログプレッソサーバー経由でセントリーをデプロイするには、バージョン2312.0以上が必要です。以前のバージョンでは手動デプロイのみサポートされます。

#### セントリーのインストール

ターゲットサーバーにセントリーをインストールするには、以下の2つの主要なステップがあります。

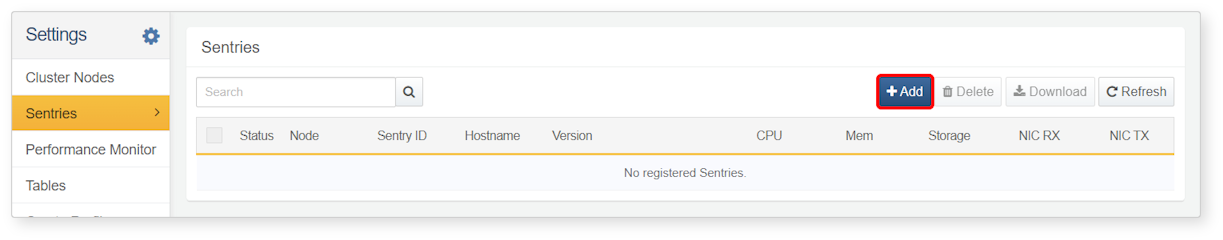
* セントリーの作成
* サーバー上でセントリーインストールコマンドの実行

インストールコマンドには、セントリーの識別子、ターゲットサーバー情報、証明書発行およびホスト認証に使用する認証トークン情報が含まれます。コマンドはホストのOSに応じて生成されます（LinuxはBash、WindowsはPowerShell）。ホスト上でコマンドを実行すると、セントリーおよびJREが自動的にインストールされ、サーバーとの接続が確立されます。

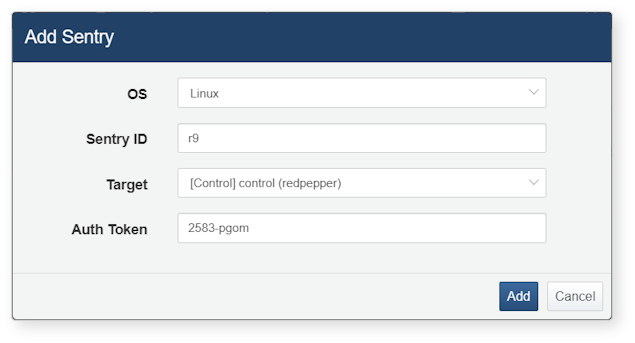
ステップ1: セントリーの作成

セントリーを作成するには:

**設定 > セントリー** で、ツールバーの **追加** をクリックします。

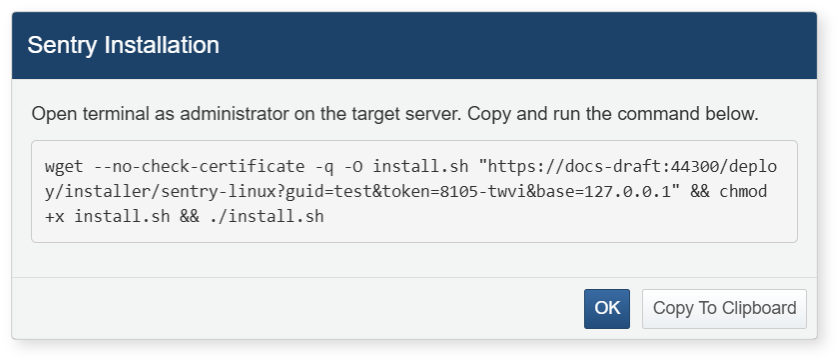


**セントリー追加** ダイアログボックスで、セントリーインストールに必要な情報を入力し、**追加** をクリックします。



* **OS**: セントリーをインストールするホストのOS（**Linux** または **Windows**）
* **セントリーID**: セントリーを識別するための一意のID
* **ターゲット**: セントリーが接続するサーバー。**設定 > クラスター** に登録されたクラスター（サーバー）ノードのリストが表示されます。
* **認証トークン**: セントリーインストール用にランダムに割り当てられる認証トークン（例: 9425-tnsa）

**セントリー追加** メッセージの指示に従い、インストールコマンドをコピーし、インストール先ホストの管理者権限ターミナルで実行します。



* **クリップボードにコピー** をクリックすると、インストールコマンドがPCのクリップボードにコピーされます。
* **OK** をクリックしてウィンドウを閉じます。

Linuxの場合

Linux用インストールコマンドはbashシェルで実行します。コマンドの書式は以下の通りで、大文字部分は生成時に自動的に割り当てられます。

# ADDR\_1: セントリーパッケージおよび証明書を配布するサーバーのアドレス# GUID: セントリーID# TOKEN: 認証トークン# ADDR\_2: セントリーと通信するサーバーのアドレス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

Linuxでwgetの代わりにcurlを使用する場合:

# ADDR\_1: セントリーパッケージおよび証明書を配布するサーバーのアドレス# GUID: セントリーID# TOKEN: 認証トークン# ADDR\_2: セントリーと通信するサーバーのアドレス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

Windowsの場合

Windows用インストールコマンドは以下の書式で、大文字部分は生成時に自動的に割り当てられます。

# ADDR\_1: セントリーパッケージおよび証明書を配布するサーバーのアドレス# GUID: セントリーID# TOKEN: 認証トークン# ADDR\_2: セントリーと通信するサーバーのアドレス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

ログプレッソサーバーが提供するインストールコマンドは、すべてのWindowsシステムに標準搭載されているPowerShell 5.1用に設計されています。PowerShellのバージョンが5.1以上の場合は、以下のように実行してください。

# ADDR\_1: セントリーパッケージおよび証明書を配布するサーバーのアドレス# GUID: セントリーID# TOKEN: 認証トークン# ADDR\_2: セントリーと通信するサーバーのアドレス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

コマンドライン実行が可能なPowerShellのバージョンは5.1であり、Windowsには標準で含まれています。Windows Terminalでは「Windows PowerShell」と表示されるものが5.1、それ以降のバージョンは単に「PowerShell」と表示されます。PowerShellを起動する際は、必ずバージョンを確認し、正しい環境で実行してください。

ステップ2: セントリーのデプロイ

コピーしたコマンドを、セントリーをインストールしたいターゲットホストで実行します。コマンド実行後、セントリーは自動的にインストールされ、起動します。

インストールディレクトリは、Linuxセントリーの場合 /opt/logpresso-sentry、Windowsセントリーの場合 C:\Program Files\Logpresso Sentry です。

Linuxの場合

事前に **net-tools**、**unzip**、**wget** がインストールされていることを確認してください。未インストールの場合は、以下のコマンドでインストールします。

# unzip, wgetはセントリーインストールに必要です。 # net-toolsはシステム情報収集に必要です。 # RHELの場合 sudo dnf install net-tools unzip wget # Debianの場合 sudo apt-get install net-tools unzip wget

bashシェルで **[ステップ1: セントリーの作成](section-sentries#outline9)** で生成したコマンドラインを **root** 権限で実行します。

ログプレッソサーバーで以下のコマンドを実行し、セントリーサービスの状態を確認できます。

systemctl status logpresso-Sentry.service

[セントリーの接続状態](https://docs.logpresso.comnull) を確認してください。セントリーの接続状態が緑色で表示されない場合は、ローカルファイアウォールやネットワーク通信状況を確認してください。

Windowsの場合

管理者権限でPowerShellを開き、**[ステップ1: セントリーの作成](section-sentries#outline9)** で生成したコマンドラインを実行します。

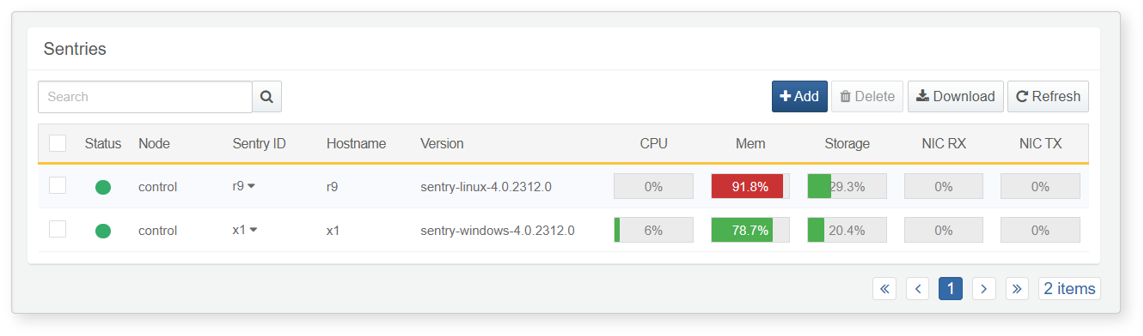
**タスクマネージャー** の **サービス** タブで **Logpresso** サービスが **実行中** であることを確認します。Windows PowerShellで以下のコマンドでも状態を確認できます。

sc.exe query Logpresso

ログプレッソ内で [セントリーの接続状態](https://docs.logpresso.comnull) を確認してください。セントリーの接続状態が緑色で表示されない場合は、ローカルファイアウォールやネットワーク通信状況を確認してください。

#### セントリーの状態確認

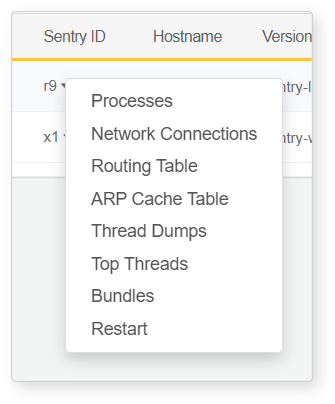
セントリーリストで各セントリーの状態を確認できます。

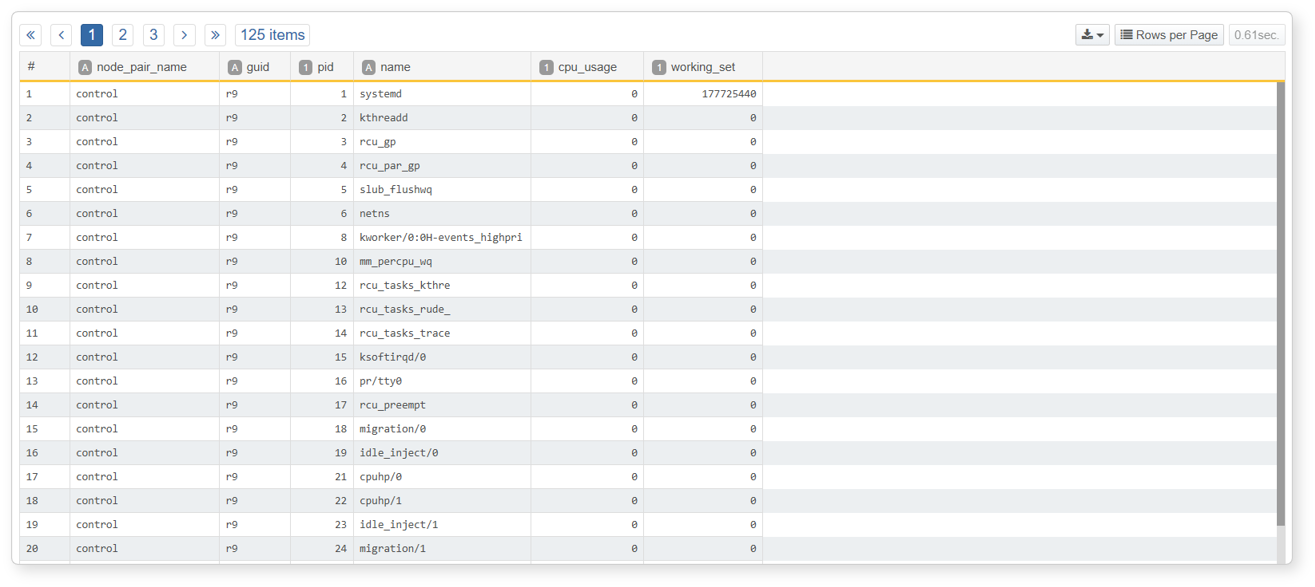
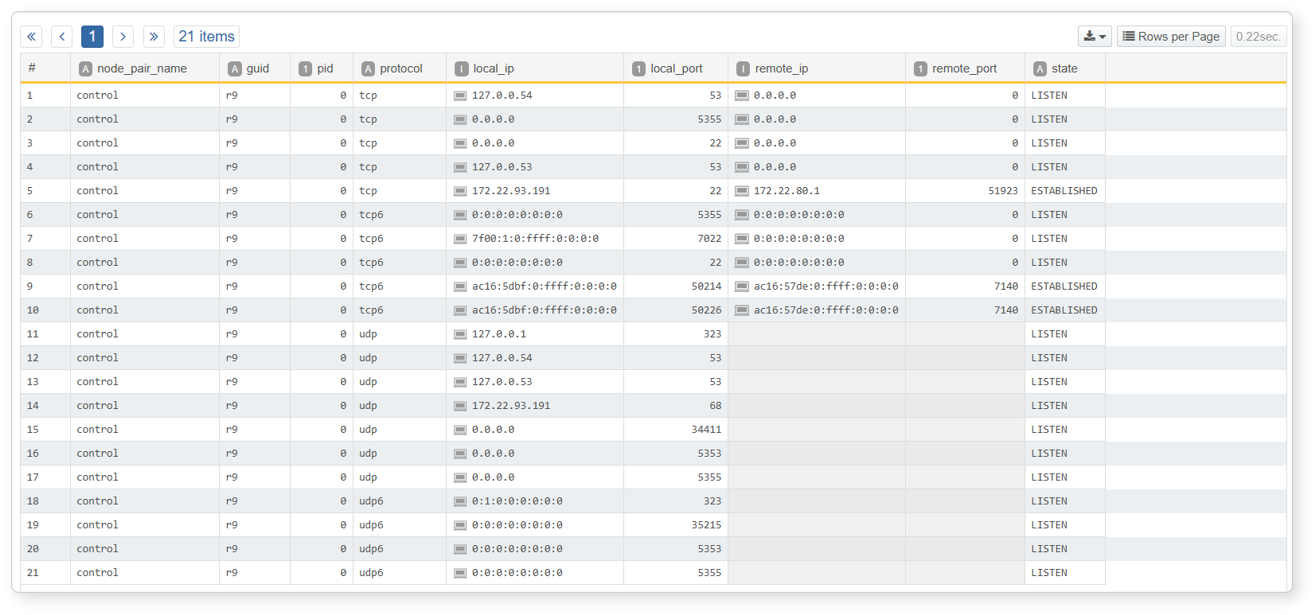
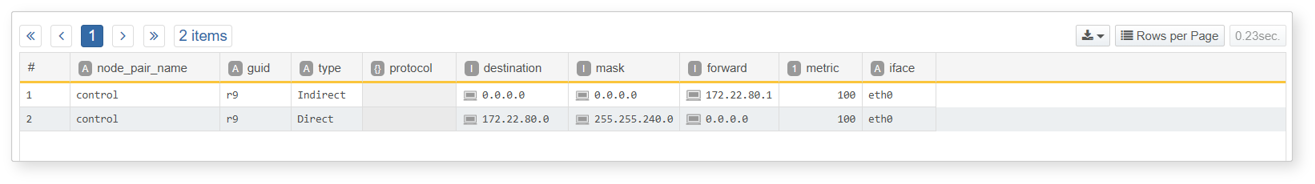
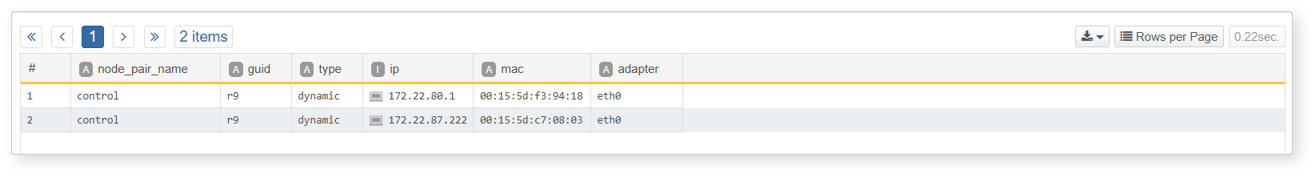
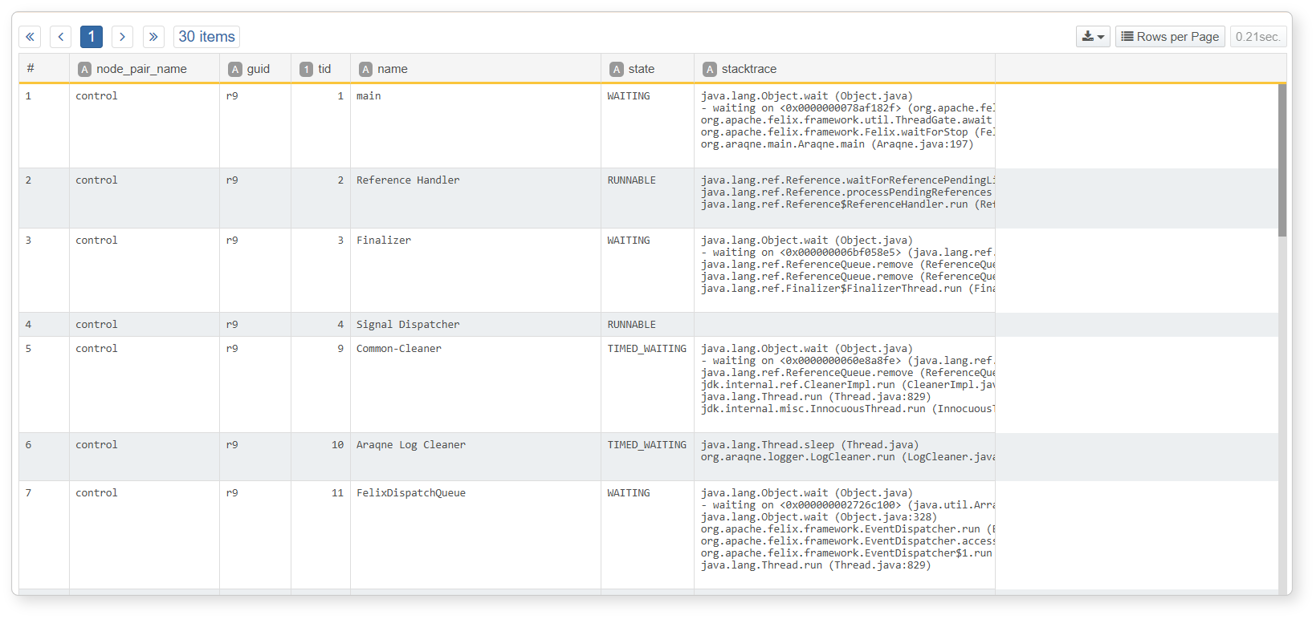
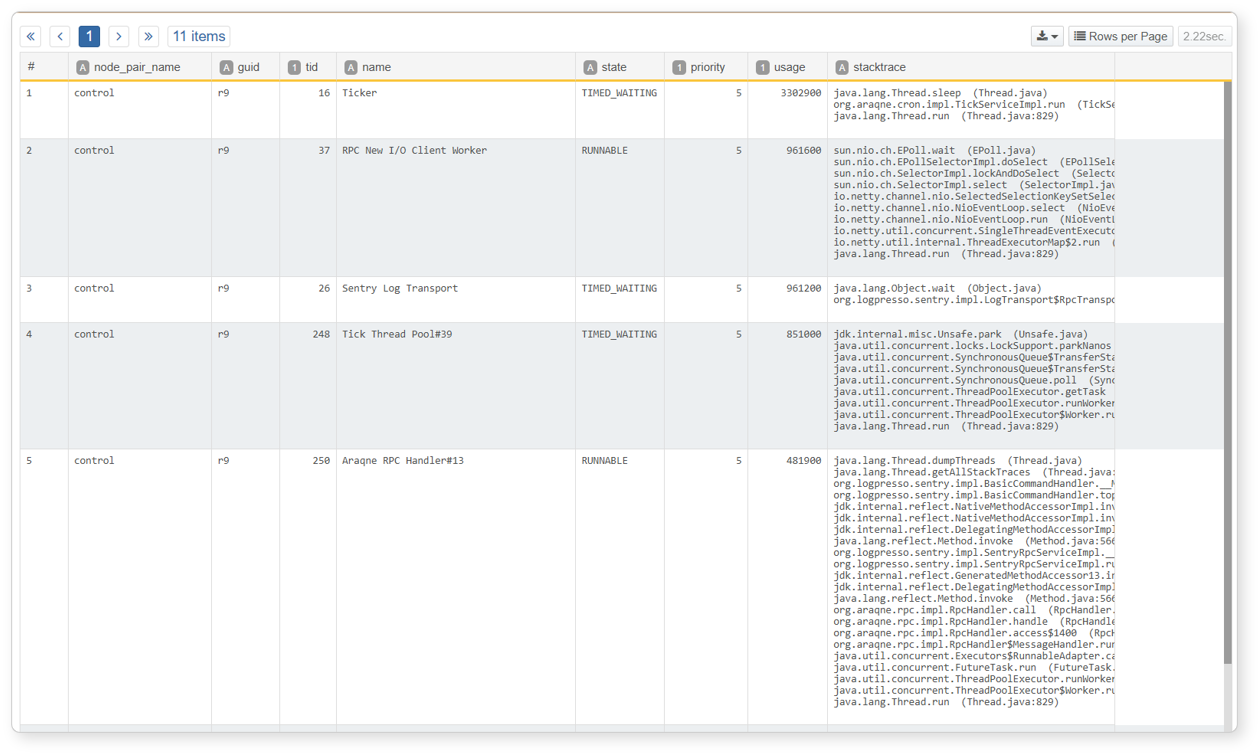
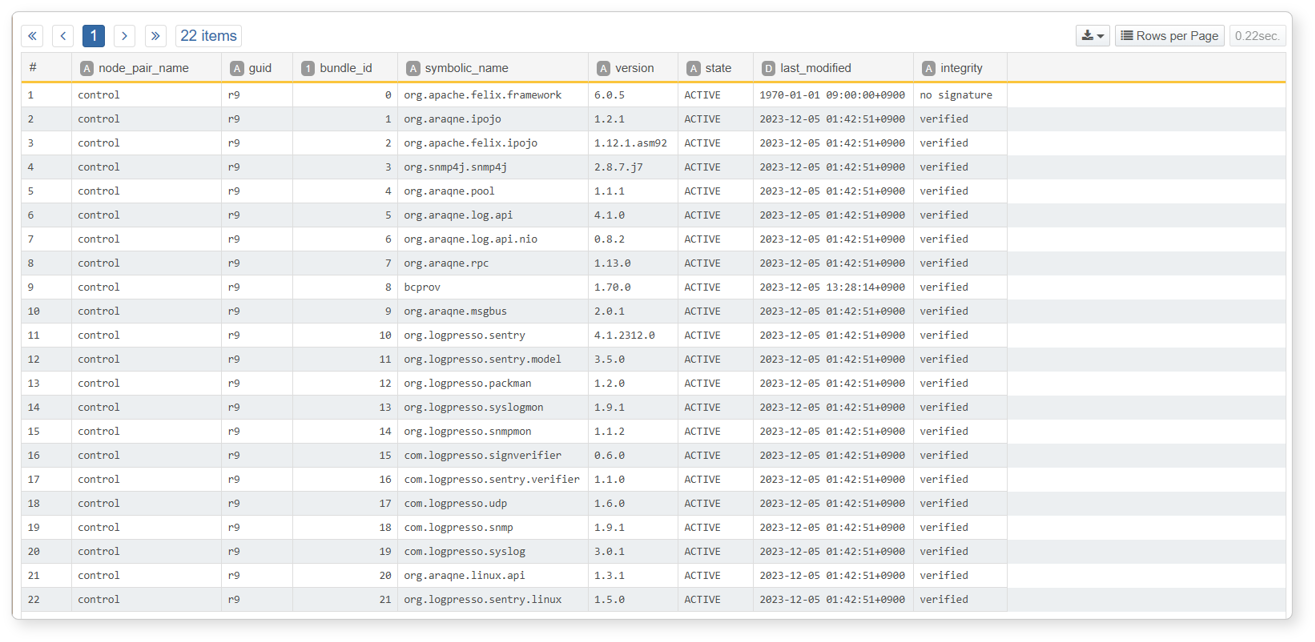


* **状態**: サーバーに接続されていれば **緑色**、未接続の場合は **グレー** で表示されます。
* **ノード**: セントリーを制御するクラスターのノード識別子。データノードは **data**、コントロールノードは **control** と表示されます。
* **セントリーID**: セントリーID
* **ホスト名**: セントリーがインストールされているホスト名
* **バージョン**: セントリーバージョン
* **CPU**: CPU使用率（%）
* **MEM**: メモリ使用率（%）
* **ストレージ**: ディスク使用率（%）。複数のストレージパーティションがある場合は最大値が表示されます。
* **NIC RX**: NIC RX帯域使用率（%）。複数のネットワークインターフェースがある場合は最大値が表示されます。
* **NIC TX**: NIC TX帯域使用率（%）。複数のネットワークインターフェースがある場合は最大値が表示されます。

#### セントリーのリモート管理

セントリーIDをクリックすると、リモート管理機能にアクセスできます。セントリーホストのプロセスリスト、ネットワーク接続情報、ルーティングテーブル、ARPキャッシュ、スレッドダンプ情報、バンドルリストの表示や、セントリーの再起動が可能です。



* **プロセス**: セントリーホスト上のプロセスリストを表示します。
* **ネットワーク接続**: セントリーホストが接続しているネットワークセッションのリストを表示します。
* **ルーティングテーブル**: セントリーホストのルーティングテーブルを表示します。
* **ARPキャッシュテーブル**: セントリーホストのARPキャッシュを表示します。
* **スレッドダンプ**: セントリー実行中に使用されているスレッドのリストを表示します。
* **トップスレッド**: スレッドごとのシステム負荷を表示します。
* **バンドル**: セントリーにインストールされているバンドルのリストを表示します。
* **再起動**: セントリーを再起動します。

#### セントリーのアンインストール

セントリーを完全にアンインストールするには、まず管理対象ホストからセントリーを削除し、ログプレッソサーバーに登録されたセントリー情報も削除します。

ステップ1: セントリーアンインストールコマンドの実行

Linuxの場合

Linuxホストでセントリーをアンインストールするには、**root** 権限でbashシェルを開き、以下のコマンドを実行します。

# セントリーの停止とアンインストールsudo systemctl stop logpresso-Sentry.servicecd /opt/logpresso-Sentrysudo ./logpresso uninstall Sentrysudo rmdir "$PKGDIR"

Windowsの場合

Windowsホストでセントリーをアンインストールするには、管理者権限でPowerShellを開き、以下のコマンドを実行します。

# Logpressoサービスの停止sc.exe stop Logpresso# Logpressoの状態確認sc.exe query Logpresso# Logpressoサービスの削除sc.exe delete Logpresso# レジストリキーの削除$reg="HKLM:\\SOFTWARE\\WOW6432Node\\Apache Software Foundation\\Procrun 2.0\\Logpresso\\"Remove-Item -Path $reg -Recurse# セントリーファイルとフォルダの削除Set-Location "C:\Program Files\Logpresso Sentry\"# 以下の行を実行し、質問にはYで回答してください。cmd.exe /c logpresso.cmd uninstall SentrySet-Location ..Remove-Item -Recurse -Path "C:\Program Files\Logpresso Sentry"

ステップ2: ログプレッソサーバーからセントリーを削除

ログプレッソサーバーからセントリーを削除するには:

**システム > セントリー** に移動し、削除したいセントリーのチェックボックスをオンにします。

ツールバーの **削除** をクリックします。

**セントリー削除** ダイアログボックスで **OK** をクリックして削除を確定します。削除しない場合は **キャンセル** をクリックしてください。

