## 릴리스 3.10.2207.0

araqne-core 버전이 3.8.0으로 업데이트되었습니다. 제품을 패치할 때 araqne-core도 함께 업데이트해야 합니다. 로그프레소 서버를 구동하려면 JDK 11을 사용해야 합니다. 센트리를 구동하려면 JDK 7 이상이 필요합니다.

### 신규 기능

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [ENT#4125](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4125) | HTTP 모니터 수집기 추가 |
| [ENT#4168](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4168) | 선재소프트 골디락스 JDBC 드라이버 지원 |

### 기능 개선

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [ENT#1684](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT1684) | Netty 버전 업데이트 |
| [ENT#3551](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3551) | CEF 파서 V25 버전 명세 지원 |
| [ENT#3700](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3700) | 쿼리창 크기 조정 기능 추가 |
| [ENT#3878](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3878) | 센트리 iPOJO 버전 업데이트 |
| [ENT#3966](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3966) | RPC TLS 취약점 제거 |
| [ENT#4027](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4027) | 웹 서버 TLS 취약점 제거 |
| [ENT#4195](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4195) | 하둡 관련 모듈 제거 |
| [ENT#4227](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4227) | 서버, 센트리 JDK 지원 버전 변경 |

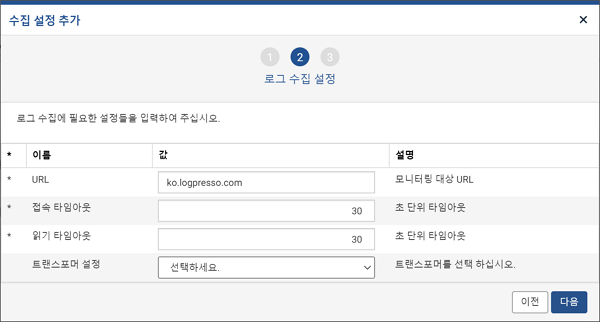
### 버그 해결

|  |  |
| --- | --- |
| 식별자 | 항목 |
| [ENT#3278](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3278) | PCAP 패킷 수집기에 유효하지 않은 패킷 필터 설정 시 프로세스가 크래시되는 현상 해결 해결 |
| [ENT#3705](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3705) | 파서 생성/편집 화면에서 커서가 이동하지 않는 현상 해결 |
| [ENT#3862](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3862) | ThreadLocal 객체 누적으로 인한 성능 저하 해결 |
| [ENT#3899](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3899) | 스트림 쿼리 생성 직후 수집기 시작 시 스트림 출력 누수 현상 해결 |
| [ENT#3931](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT3931) | JDK 11 환경에서 윈도우 센트리에 araqne.rpc.client.oio 부팅 옵션 사용 시 연결 실패하는 현상 해결 |
| [ENT#4069](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4069) | CEF 파서 역슬래시 다음 문자가 유실되는 현상 해결 |
| [ENT#4092](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4092) | row 레이아웃 테이블에 대해 fulltext 쿼리 시 인메모리 데이터가 항상 오름차순으로 출력되는 현상 해결 |
| [ENT#4137](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4137) | 서브쿼리에서 parsemap 커맨드 실행 시 field 옵션을 인식하지 못하는 현상 해결 |
| [ENT#4162](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4162) | 테이블 저장 경로 지정 시 오류 발생 해결 |
| [ENT#4171](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4171) | 유닉스 센트리 SNMP 번들이 시작 실패하는 현상 해결 해결 |
| [ENT#4252](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4252) | CEF 로그의 cn 필드가 값이 없는 경우 CEF 파서가 파싱에 실패하는 현상 해결 |
| [ENT#4240](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4240) | SNMPv3 인터페이스 통계 수집기 수집 실패 해결 |
| [ENT#4266](https://docs.logpresso.com/ko/enterprise/3.10/issues/ENT4266) | table 쿼리 커맨드에서 meta() 함수 사용 시 쿼리 오류가 발생하는 현상 해결 |

### 상세 내역

#### ENT#4125 HTTP 모니터 수집기 추가

HTTP/HTTPS 웹 서버 상태를 모니터링하는 수집기가 추가되었습니다.



입력값은 다음과 같습니다.

* 모니터링할 URL
* 접속 타임아웃 (초)
* 읽기 타임아웃 (초)

수집되는 필드는 다음과 같습니다.

* \_time (날짜/시각): HTTP/HTTPS 접속을 시도한 시각
* url (문자열): 접속 대상 URL
* dst\_ip (IP 주소): 웹서버 IP
* status (32비트 정수): 응답 코드. 정상인 경우 200, 그 외 301, 401, 404, 500 등 코드
* elapsed (32비트 정수): 접속 시도 후 경과된 밀리 초 단위 시간
* hostname (문자열): 수집기를 구동하는 호스트명 (센트리이면 센트리 호스트명)
* rcvd\_bytes (64비트 정수): 수신한 본문 바이트 수

#### ENT#1684 Netty 버전 업데이트

Netty 버전을 3.10.4.Final에서 4.1.75.Final로 업데이트했습니다.

#### ENT#3551 CEF 파서 V25 버전 명세 지원

예를 들어 벡트라 CEF 로그는 아래와 같은 키, 값 쌍을 포함합니다.

flexNumber1Label=threat flexNumber1=52 flexNumber2Label=certainty flexNumber2=70

이전에는 flexNumber 필드를 파싱할 때 Label 필드를 참조하지 않아 모두 개별적인 필드로 파싱되었습니다. 패치 반영 후에는 위의 예시를 파싱했을 때 threat 필드의 64비트 정수 값 52와, certainty 필드의 64비트 정수 값 70이 추출됩니다.

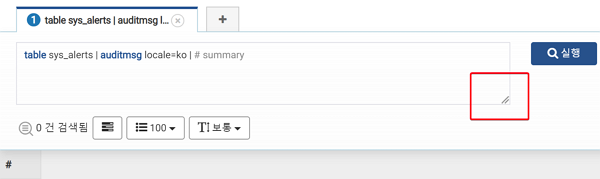
CEF 로그 파서는 이 패치를 통해 Micro Focus Security ArcSight Common Event Format Version 25 문서에 명시된 아래의 필드를 추가로 인식합니다.

|  |  |  |  |
| --- | --- | --- | --- |
| CEF 키 | 전체 이름 | 데이터 타입 | 길이 |
| c6a1 | deviceCustomIPv6Address1 | IPv6 주소 |  |
| c6a1Label | deviceCustomIPv6Address1Label | 문자열 | 1023 |
| c6a3 | deviceCustomIPv6Address3 | IPv6 주소 |  |
| c6a3Label | deviceCustomIPv6Address3Label | 문자열 | 1023 |
| c6a4 | deviceCustomIPv6Address4 | IPv6 주소 |  |
| c6a4Label | deviceCustomIPv6Address4Label | 문자열 | 1023 |
| cfp1 | deviceCustomFloatingPoint1 | 64비트 실수 |  |
| cfp1Label | deviceCustomFloatingPoint1Label | 문자열 | 1023 |
| cfp2 | deviceCustomFloatingPoint2 | 64비트 실수 |  |
| cfp2Label | deviceCustomFloatingPoint2Label | 문자열 | 1023 |
| cfp3 | deviceCustomFloatingPoint3 | 64비트 실수 |  |
| cfp3Label | deviceCustomFloatingPoint3Label | 문자열 | 1023 |
| cfp4 | deviceCustomFloatingPoint4 | 64비트 실수 |  |
| cfp4Label | deviceCustomFloatingPoint4Label | 문자열 | 1023 |
| deviceCustomDate1 | deviceCustomDate1 | 날짜 |  |
| deviceCustomDate1Label | deviceCustomDate1Label | 문자열 | 1023 |
| deviceCustomDate2 | deviceCustomDate2 | 날짜 |  |
| deviceCustomDate2Label | deviceCustomDate2Label | 문자열 | 1023 |
| flexNumber1 | flexNumber1 | 정수 |  |
| flexNumber1Label | flexNumber1Label | 문자열 |  |
| flexNumber2 | flexNumber2 | 정수 |  |
| flexNumber2Label | flexNumber2Label | 문자열 |  |
| flexDate1 | flexDate1 | 날짜 |  |
| flexDate1Label | flexDate1Label | 문자열 | 128 |
| flexString1 | flexString1 | 문자열 | 1023 |
| flexString1Label | flexString1Label | 문자열 | 128 |
| flexString2 | flexString2 | 문자열 | 1023 |
| flexString2Label | flexString2Label | 문자열 | 128 |

#### ENT#3700 쿼리창 크기 조정 기능 추가

다음 화면에서 쿼리창 크기 조절 기능이 추가되었습니다.

* 쿼리
* 프로시저
* 스트림 쿼리
* 예약된 쿼리



#### ENT#3878 센트리 iPOJO 버전 업데이트

센트리의 iPOJO 버전을 1.12.1으로 업데이트했습니다.

#### ENT#3966 RPC TLS 취약점 제거

* TLS1, TLS1.1가 기본으로 비활성화 됩니다. 해당 TLS 버전 활성화가 필요한 경우 부팅 옵션에 -Daraqne.rpc.weak\_tls=enabled 를 추가해야 합니다.
* CBC, DH suite가 기본으로 비활성화 합니다. 해당 suite 활성화가 필요한 경우 부팅 옵션에 -Daraqne.rpc.weak\_cipher=enabled 를 추가해야 합니다.
* JDK 7 환경에서 구동 중인 센트리의 경우 JDK가 TLS 1.2 버전을 지원하지 않아, 패치 후 로그프레소 서버와 연결이 실패할 수 있습니다. 이 경우 JDK 버전을 올리는 것을 권장하지만, 일부 유닉스 서버의 경우 지원하는 최대 JDK 버전을 1.7입니다.
* 예를 들어, HP-UX Itanium 11.31 버전 미만은 JDK 8을 지원하지 않습니다. 이 경우 로그프레소 서버 부팅 옵션에 -Daraqne.rpc.weak\_tls=enabled 와 -Daraqne.rpc.weak\_cipher=enabled 를 모두 추가해서 구동하면 TLS1.1 버전도 지원하여 센트리가 정상적으로 연결됩니다.

#### ENT#4027 웹 서버 TLS 취약점 제거

* TLS1, TLS1.1가 기본으로 비활성화 됩니다. 해당 TLS 버전 활성화가 필요한 경우 부팅 옵션에 -Daraqne.httpd.weak\_tls=enabled 를 추가해야 합니다.
* CBC, DH suite가 기본으로 비활성화 됩니다. 해당 suite 활성화가 필요한 경우 부팅 옵션에 -Daraqne.httpd.weak\_cipher=enabled 를 추가해야 합니다.
* TLS 접속 시 2048 비트 이상의 DH 그룹으로 강제하여 LOGJAM ([CVE-2015-4000](https://github.com/advisories/GHSA-v98w-p8f7-9qqf)) 취약점을 해결했습니다.
* TLS 접속 시 CBC 암호화를 금지하여 LUCKY13 ([CVE-2013-0169](https://github.com/advisories/GHSA-pg96-42c4-p633)) 취약점을 해결했습니다.

#### ENT#4195 하둡 관련 모듈 제거

하둡 관련 모듈이 번들 목록에서 제거되었습니다. 추후 하둡 관련 쿼리 및 수집을 하려면 별도 하둡 앱을 설치하세요. (로그프레소 스토어에 공개 예정)

#### ENT#4168 선재소프트 골디락스 JDBC 드라이버 지원

지원하는 JDBC 드라이버 목록에 선재소프트 골디락스 JDBC 드라이버가 추가되었습니다.

#### ENT#4227 서버, 센트리 JDK 지원 버전 변경

엔터프라이즈 서버가 자바 11 빌드로 전환됨에 따라 JDK 최소 지원 버전이 JDK 8에서 **JDK 11**로 변경되었습니다. 센트리의 JDK 최소 지원 버전은 JDK 6에서 **JDK 7**로 변경되었습니다. jemalloc 패치된 JDK 11 버전은 CentOS 혹은 RHEL 6.x 환경에서 동작하지 않으므로, 해당 환경에서 제품을 업그레이드하려면 운영체제도 업그레이드해야 합니다.

#### ENT#3278 PCAP 패킷 수집기에 유효하지 않은 패킷 필터 설정 시 프로세스가 크래시되는 현상 해결

PCAP 패킷 수집기 생성 시 패킷 필터 항목에 입력한 값이 버클리 패킷 필터(BPF) 문법에 맞지 않는 값이면 수집기를 시작하자마자 로그프레소가 강제 종료되는 현상을 해결했습니다.

#### ENT#3705 파서 생성/편집 화면에서 커서가 이동하지 않는 현상 해결

파서 생성/편집 화면에서 필수 항목을 클릭한 후 값을 입력하지 않으면 다른 항목으로 커서가 이동하지 않는 현상을 해결했습니다.

#### ENT#3862 ThreadLocal 객체 누적으로 인한 성능 저하 해결

JDK 11의 Full GC 회피 최적화로 인해 ThreadLocal 객체 누적으로 성능이 저하되는 현상을 해결했습니다. 스트림 처리 성능 저하로 시스로그 수집 지연 현상이 발생할 수 있고, 이전 버전에서는 주기적으로 perf.gc를 수행하는 방법으로 우회할 수 있습니다. 패치 후에는 강제로 GC를 수행하지 않아도 ThreadLocal 객체가 누적되지 않습니다.

#### ENT#3899 스트림 쿼리 생성 직후 수집기 시작 시 스트림 출력 누수 현상 해결

수집기 데이터소스 스트림 쿼리를 생성한 직후 (100ms 이내) 수집기를 시작하면 스트림 출력이 누수되는 현상을 해결했습니다.

#### ENT#3931 JDK 11 환경에서 윈도우 센트리에 araqne.rpc.client.oio 부팅 옵션 사용 시 연결 실패하는 현상 해결

JDK 11 환경에서 윈도우 센트리에 -Daraqne.rpc.client.oio=enabled 부팅 옵션을 사용하면 로그프레소 서버에 접속 실패하는 현상을 해결했습니다.

이전 버전에서 이와 같은 문제로 로그프레소 서버에 연결에 실패하면 araqne.log에 Unexpected leftover data after 오류가 출력됩니다:

[2021-01-04 17:34:35,590] WARN (AraqneLogService) - [org.jboss.netty.handler.ssl.SslHandler] Unexpected leftover data after SSLEngine.unwrap(): status=OK handshakeStatus=NEED\_WRAP consumed=0 produced=0 remaining=2197 data=1403030001011703...omitted.....[2021-01-04 17:34:40,576] WARN (RpcHandler) - araqne rpc: ssl handshake failure, closing [/xxx.xxx.xxx.xxx:7140][2021-01-04 17:34:40,578] INFO (ConnectionWatchdogImpl) - logpresso-sentry: failed to connect, closing connectionjava.lang.RuntimeException: rpc-ssl connection failed at org.araqne.rpc.RpcClient.connectSsl(RpcClient.java:179) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_connect(ConnectionWatchdogImpl.java:214) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.connect(ConnectionWatchdogImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_checkConnections(ConnectionWatchdogImpl.java:156) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.checkConnections(ConnectionWatchdogImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_checkNow(ConnectionWatchdogImpl.java:134) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.checkNow(ConnectionWatchdogImpl.java) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.\_\_run(ConnectionWatchdogImpl.java:111) at org.logpresso.sentry.impl.ConnectionWatchdogImpl.run(ConnectionWatchdogImpl.java) at java.base/java.lang.Thread.run(Thread.java:834)Caused by: javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated at java.base/sun.security.ssl.SSLSessionImpl.getPeerCertificates(SSLSessionImpl.java:556) at org.araqne.rpc.RpcClient.connectSsl(RpcClient.java:167) ... 9 more

#### ENT#4069 CEF 파서 역슬래시 다음 문자가 유실되는 현상 해결

CEF 파서 파싱 결과에서 역슬래시(\) 다음 문자가 유실되는 현상을 해결했습니다. 예를 들어 아래 로그의 경우 다음과 같이 파싱되었습니다.

|  |  |
| --- | --- |
| 구분 | 로그/결과 |
| 원본 로그 | cs5="C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /dde |
| 기존 파싱 결과 | "C:\rogram Files (x86)\icrosoft Office\ffice16\XCEL.EXE" /dde |
| 패치 후 파싱 결과 | "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /dde |

#### ENT#4092 row 레이아웃 테이블에 대해 fulltext 쿼리 시 인메모리 데이터가 항상 오름차순으로 출력되는 현상 해결

row 레이아웃의 테이블에서 아직 디스크에 기록되지 않고 인메모리에 있는 데이터에 대해 fulltext 검색을 수행할 경우, fulltext order 옵션과 관계없이 항상 오름차순(asc)으로 출력되는 현상을 해결했습니다.

#### ENT#4137 서브쿼리에서 parsemap 커맨드 실행 시 field 옵션을 인식하지 못하는 현상 해결

서브쿼리에서 parsemap 커맨드 사용 시 field 옵션을 사용해도 인식하지 못하고 쿼리 오류가 발생하던 현상을 해결했습니다.

#### ENT#4162 테이블 저장 경로 지정 시 오류 발생 해결



테이블 생성 시 테이블 저장 디렉터리를 별도로 설정하여 데이터를 입력하면 다음 오류 로그가 발생하던 현상이 해결 되었습니다.

ERROR (LogCounterV3) - logpresso logstorage: cannot count, invalid .idx file (too short)

또한, ENT-3.10.2203.0 배포 버전에서 2차 스토리지에만 데이터가 존재하는 경우에도 동일한 오류가 발생하여 현 배포 버전에서 추가로 해결하였습니다.

#### ENT#4171 유닉스 센트리 SNMP 번들이 시작 실패하는 현상 해결

유닉스 운영체제에서는 ENT-3.10.2203.0 배포 버전에서 업데이트 된 SNMP 번들의 iPOJO 의존성이 충족되지 않는 문제로 SNMP 번들을 시작할 수 없었습니다. 따라서 SNMP 번들에서 iPOJO 1.10.0 버전을 참조하도록 수정하여 해결하였습니다.

#### ENT#4240 SNMPv3 인터페이스 통계 수집기 수집 실패 해결

ENT-3.10.2203.0 배포 버전에서 SNMPv3 인터페이스 통계 수집기 실행 시 아래 오류 로그가 발생하고 데이터가 수집되지 않던 현상을 해결했습니다.

[2022-05-09 11:24:01.608] WARN (SnmpV3InterfaceLogger) - SNMP query failed for xxx.xxx.xxx.xxx:161, msg: java.lang.NullPointerException(Context engine ID must not be null)[2022-05-09 11:24:01.608] DEBUG (SnmpV3InterfaceLogger) - SNMP query failed exception detailjava.lang.NullPointerException: Context engine ID must not be null at org.snmp4j.ScopedPDU.setContextEngineID(ScopedPDU.java:69) at org.snmp4j.util.DefaultPDUFactory.applyContextInfoToScopedPDU(DefaultPDUFactory.java:118) at org.snmp4j.util.DefaultPDUFactory.createPDU(DefaultPDUFactory.java:103) at org.snmp4j.util.TreeUtils.walk(TreeUtils.java:171) at org.snmp4j.util.TreeUtils.getSubtree(TreeUtils.java:141) at org.logpresso.snmpmon.SnmpV3InterfaceLogger.query(SnmpV3InterfaceLogger.java:430) at org.logpresso.snmpmon.SnmpV3InterfaceLogger.runOnce(SnmpV3InterfaceLogger.java:240) at org.araqne.log.api.AbstractLogger$DefaultLoggerTask.run(AbstractLogger.java:677) at java.base/java.lang.Thread.run(Thread.java:834)

#### ENT#4252 CEF 로그의 cn 필드 값이 없는 경우 CEF 파서가 파싱에 실패하는 현상 해결

CEF 로그의 cn1Label, cn2Label, cn3Label 필드에 값이 있는데 cn1, cn2, cn3 필드에 값이 없는 경우 CEF 파서가 파싱에 실패하는 현상을 해결했습니다. 패치 후에는 CEF 파서가 값이 없거나 파싱되지 않는 필드는 제외하고 나머지 필드를 정상적으로 파싱합니다.

#### ENT#4266 table 쿼리 커맨드에서 meta() 함수 사용 시 쿼리가 실패하는 현상 해결

table 쿼리 커맨드 실행 시 meta() 함수를 사용할 경우 쿼리 오류가 발생하면서 쿼리가 실행되지 않는 현상을 해결했습니다. 쿼리 오류 발생 시 아래 오류 로그가 발생합니다.

araqne logdb: cannot create queryjava.lang.UnsupportedOperationException: set table-metadata matcher as not-optional is not supported at org.araqne.logdb.query.parser.TableParser$MetaS.setOptional(TableParser.java:451) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_expandToLocalStorageObjectSpec(DistributedQueryPlanner.java:1221) at com.logpresso.query.planner.DistributedQueryPlanner.expandToLocalStorageObjectSpec(DistributedQueryPlanner.java) at com.logpresso.query.planner.DistributedQueryPlanner.\_\_M\_expandToLocalStorageObjectSpecs(DistributedQueryPlanner.java:1193) at com.logpresso.query.planner.DistributedQueryPlanner.expandToLocalStorageObjectSpecs(DistributedQueryPlanner.java)