nurit

빅 데이터 실시간 로그 수집을 위한

BaroCollector 솔루션 소개서

2021. 6.

Content

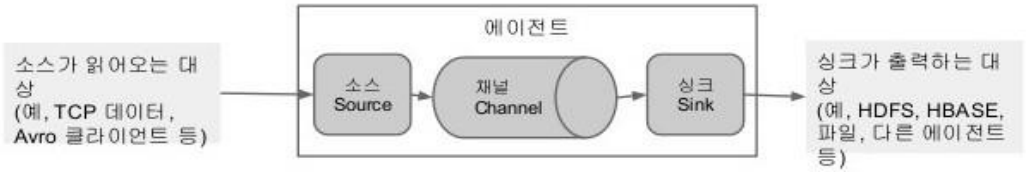
nurit

Ⅰ. 솔루션 개요

BaroCollector 란

- **BaroCollector는 Apache Flume 기반으로 J2EE환경에서 Customizing.**
- **BaroCollector는 다양한 Source에서 발생된 많은 양의 로그 데이터를 중앙의 데이터 저장소로 효율적으로 수집해 주는 분산처리, 신뢰성, 가용성을 갖춘 로그 수집기.**

BaroCollector 기본구성



- 소스: 지정한 소스를 통해서 이벤트를 받아 채널로 전달
- 채널: 이벤트를 임시로 보관
  - 메모리 채널, 파일 채널, DB 채널
- 싱크: 채널에서 이벤트를 읽어와 출력 대상에 씀
  - 싱크가 출력 대상에 이벤트(데이터)를 전달을 완료하면, 채널에서 해당 이벤트를 삭제

nurit

II. 솔루션 특징

BaroCollector 특징

- **신뢰성**

  -지속적으로 실패하는 상황에 직면하더라도 데이터 손실 없이 데이터를 보내야 하는 특성.
  -신뢰성 수준 설정
  엔드 투 엔드 모드 (end to end)
  저장 모드 (store on failure)
  비신뢰 모드 (best effort)

- **관리성**

  -데이터 흐름을 제어하고, 모니터링 등 결과를 관리.
  -사용자는 흐름을 모니터링 할 수 있고, 즉시 재 설정 가능.
  -자동적으로 부하의 변동이나 일부 노드의 실패, 하드웨어 추가와 같은 시스템의 변화에 대한 정보 제공.

- **확장성**

  -시스템의 성능을 증가시키는 것으로 수평적 자원 확장을 지원.
  -각 계층별로 부하량에 따라 노드를 추가해서 전체적인 성능을 향상 가능.

Ⅲ. 솔루션 컴포넌트

BaroCollector 솔루션은 수집대상이 되는 Source 영역, 인터페이스를 하는 Channel 영역, 자료를 전송하는 Sink 영역 등 3개의 컴포넌트 영역으로 구분되어 있습니다.

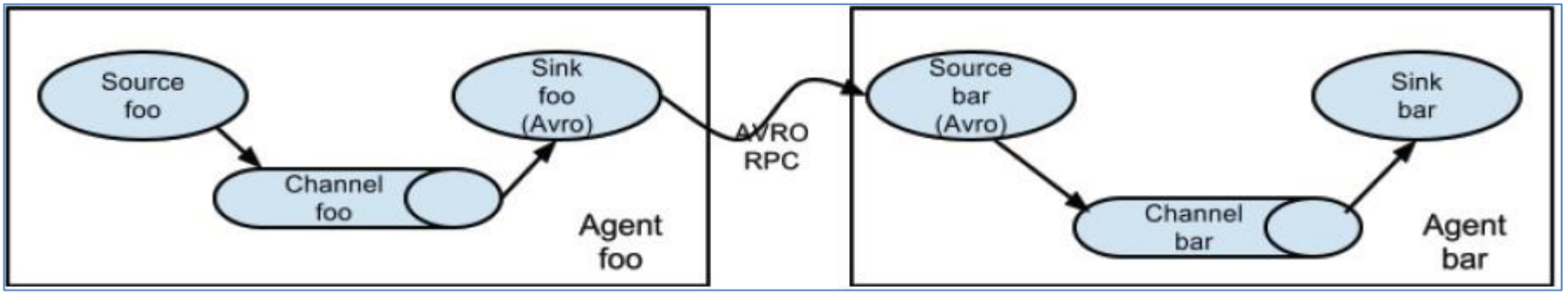
Source	Channel	Sink
Avro : Avro 프로토콜로 수집	Memory : Memory 사용	Avro : Avro 프로토콜로 전송
Thrift : Thrift 프로토콜로 수집	JDBC : DB 사용	Thrift : Thrift 프로토콜로 전송
Syslog : Syslog 프로토콜로 수집 -Syslog TCP, Multiport Syslog TCP -Syslog UDP	File : File 사용	IRC : IRC 프로토콜로 전송
HTTP : HTTP 프로토콜로 수집		ElasticSearch : Elastic에 저장
JMS : JMS 프로토콜로 수집 -Pluggable converter 지원		MorphlineSolr : Solr에 저장
NetCat : TCP/IP 데이터 수집		HDFS : HDFS에 저장
Exec : Linux 명령어로 수집		HBase : HBase에 저장 -HBaseSink, AsyncHBaseSink
Spooling Directory : 폴더에 신규로 추가된 파일 수집		Logger : 테스트 또는 디버깅을 위해 로깅
Sequence Generator : 0부터 1씩 증가하는 event 생성		File Roll : 파일로 저장
Legacy : 이전 버전의 Flume으로부터 데이터 수집 -Avro Legacy, Thrift legacy		JDBC : Database로 저장
JDBC : Database 수집		Null : 아무 일도 하지 않음
Custom	Custom	Custom

BaroCollector 주요 기능

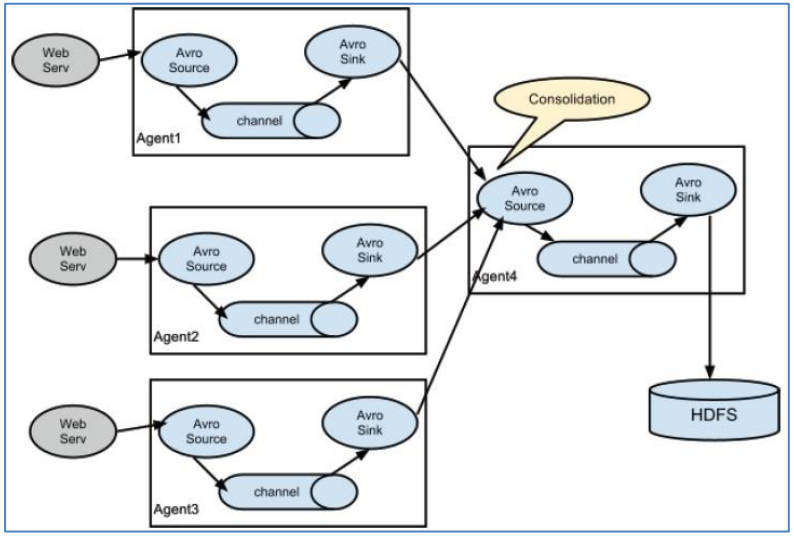
- **Interceptor**
  - -수집한 데이터를 변경 또는 삭제.
  - -종류
    삽입 : Timestamp, Host, Static, UUID
    변형/삭제 : Morphline, Regex Filtering, Regex Extractor
- **Channel Selector**
  - -Source에서 Channel로 연동시 Channel을 지정.
  - -종류
    Replicating (Default), Multiplexing, Custom
- **Sink Processor**
  - -Sink할 대상을 다중 선택.
  - -종류
    Default, Failover, Loadbalancing, Custom
  - -Sink Group : 여러 개의 Sink를 하나의 그룹으로 관리
- **Serializer / Deserializer**
  - -Serializer
    Body Text, Avro Event
  - -Deserializer
    LINE, AVRO, BlobDeserializer
- **Handler**
  - -JSONHandler, BlobHandler
- **Appender**
  - -Log4J Appender, Load Balancing Log4J Appender
- **Reporting**
  - -Ganglia, JSON, Custom
- **Plugin**
  - -$FLUME_HOME/plugins.d/플러그인명/
  - -$FLUME_HOME/plugins.d/플러그인명/lib/~.jar-
  - -$FLUME_HOME/plugins.d/플러그인명/libext/~.jar-
  - -$FLUME_HOME/plugins.d/플러그인명/native/~.so

V. 솔루션 FLOW

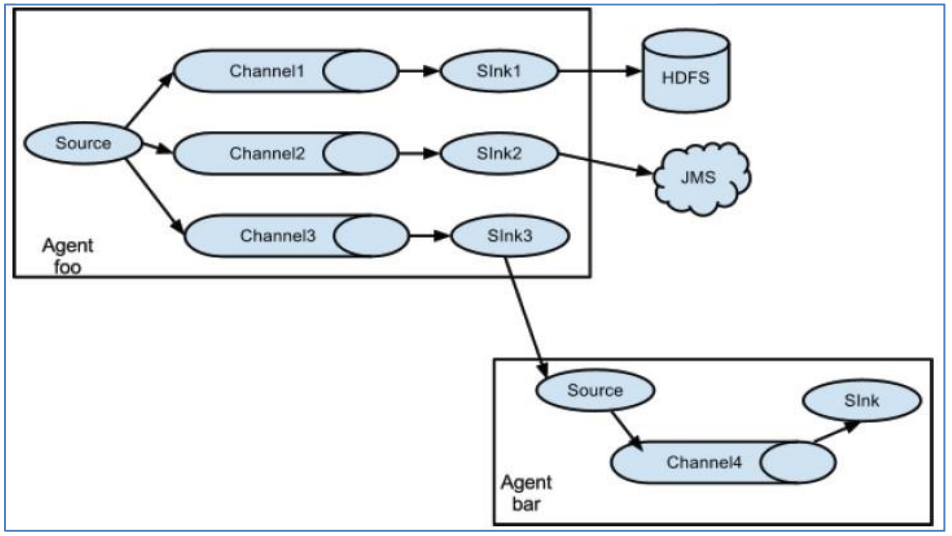
Setting multi-agent flow



Consolidation



Multiplexing the flow

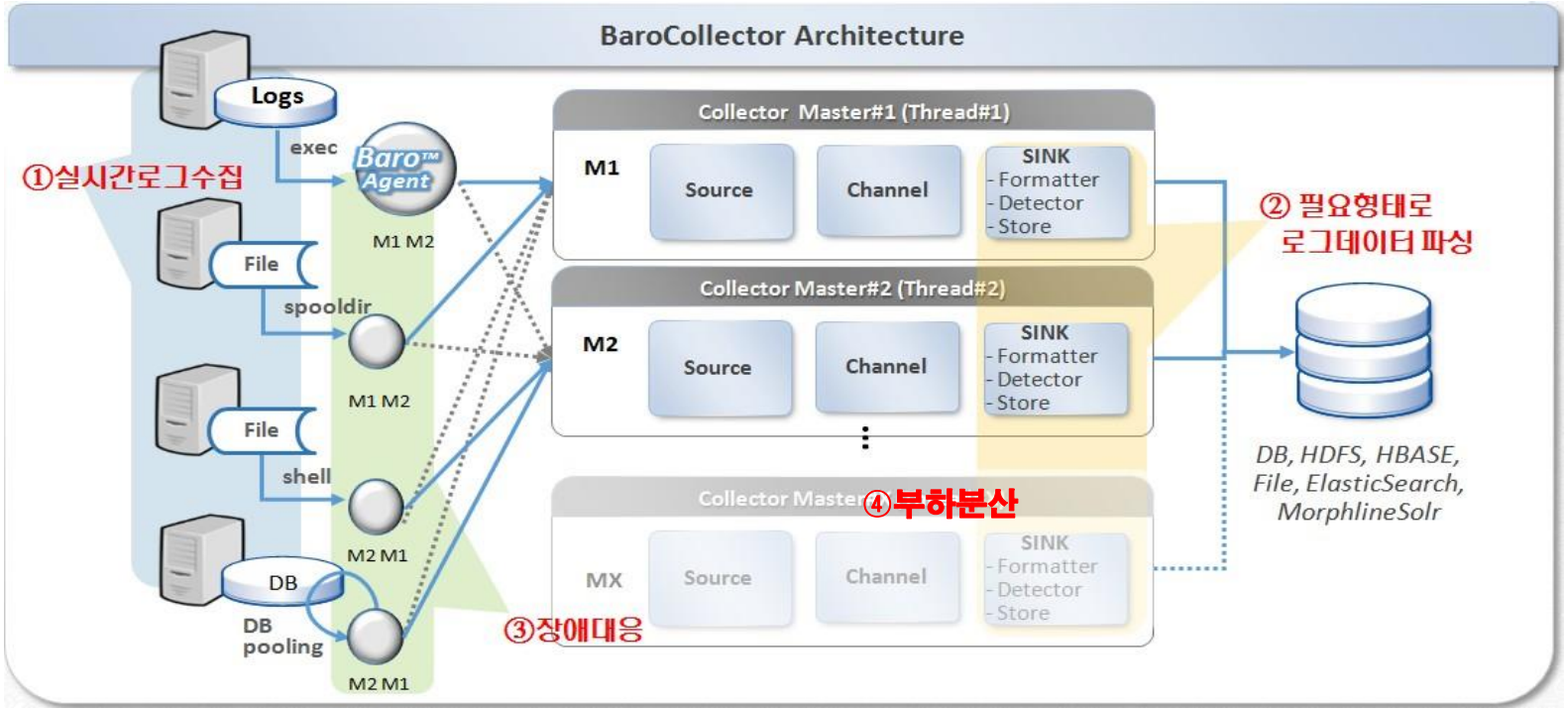


nurit

Ⅵ. 솔루션 아키텍처

BaroCollector는 기존업무에 변경을 거의 주지 않고 로그를 실시간으로 수집하고, 이를 필요한 형태로 저장이 가능하며, J2EE기반의 Collector로 어떤 환경에서든지 즉시 로그수집이 가능한 것이 특징입니다.

①**실시간로그수집**: 환경변수 설정만으로 Source 종류에 상관없이 실시간으로 수집 가능.
②**필요형태저장** : 로그 포맷터를 보유해 환경변수만으로도 비정형/정형에 상관없이 원하는 형태(JSON, Key-Value, XML, String, Delimiter)로 저장가능.
③**장애대응** : 장애 시 이를 감지하여, 다른 Thread (또는 다른 Instance)로 대체 및 비정상 종료시 재기동으로 안정적 수집가능.
④**부하분산** : 순차적 배분(Round Robin), 동적 배분(Random) 가능.



nurit

Ⅶ. 적용분야

BaroCollector 솔루션은 Stock Market, Telecom, Health & Life Science, 보안, 제조 등 빅 데이터를 실시간 로그 수집이 필요한 모든 분야에서 사용 가능합니다.

nurit

1. BaroSolution 제품군

구 분	설 명	비고
BaroPAM	정보자산의 다양한 운영체제 및 애플리케이션에서 2차 인증으로 일회용 인증키를 접목시켜 중앙 집중적 인증 메커니즘을 지원하는 단순하면서도 강력한 정보자산의 접근제어 인증 솔루션.	
BaroCARD	생체정보인 지문정보를 적용한 최적의 본인인증 솔루션으로 생체정보인 지문정보를 플라스틱 카드에 등록한 후 등록된 지문정보를 인식하면 일회용 인증키를 생성하는 카드(지문인식 기능과 인증카드를 내장한 신개념 카드) 로 지문인식 인증카드 솔루션.	
BaroCRYPT	Feistel 암호를 사용하여 크기가 작고 구현이 쉬운 블록 암호화 알고리즘인 XXTEA (Extended Extended Tiny Encryption Algorithm)를 기반으로 하는 가볍고 가장 빠른 암호화 알고리즘을 적용한 솔루션.	
BaroCollector	다양한 Source에서 발생된 많은 양의 로그 데이터(Big Data)를 중앙의 데이터 저장소로 효율적으로 수집해 주는 분산처리, 신뢰성, 가용성을 갖춘 실시간 로그 수집기.	
BaroFDS	이상금융거래탐지 및 대응업무에 대한 모금융기관의 2년간의 Know-how을 바탕으로 개발된 금융권 유일의 검증된 FDS 솔루션으로서 복잡한 금융권 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있음.	
BaroIDS	정보자산(서버, 네트워크장비, 보안장비, 저장장치, 데이터베이스, 애플리케이션, 기타)의 이상접속 탐지 및 차단에 대한 현장의 Know-how을 바탕으로 FDS(Fraud Detection System)를 적용하여 개발된 솔루션.	

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 010-2771-4076