4

|  |  |
| --- | --- |
|  | KTC-PF-OP-002 |
|  | **로그 표준화 방침** |

**플랫폼운영팀**



**개정 이력**

|  |  |  |  |
| --- | --- | --- | --- |
| **버전** | **개정일자** | **개정내용** | **작성자** |
| 0.1 | 2024-07-01 | 신규 작성 | 최기용 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **개요**

## 목적

## 본문서는 개발센터에서 개발 및 운영하는 서비스에 대한 로그 내용 및 디자인을 설명한다.

## 로그를 바탕으로 사용자의 사용 패턴 추적 및 서비스 모니터링에 사용됨을 이해한다.

## 시스템 장애에 대한 판단 및 디버깅을 이해한다.

## 로그의 구조의 이해 및 표현에 대한 관리가 가능하다.

## 로그에 나타난 각 필드 및 값의 내용을 이해한다.

## 기능의 개요

## 관리자가 원하는 LOG LEVEL을 설정하여 특정 LEVEL의 로그만을 출력하는 기능을 제공한다.

## LOG의 LEVEL에 맞게 표현된 데이터는 종류에 따라 표현 여부가 결정된다.

## 관리자는 로그파일에 대한 파일시스템 제한 설정을 함으로서 시스템 에러에 대한 대비 기능을 제공한다.

## 실시간 로그를 위해 특정 키워드를 제공하며 모니터링 서버는 이를 바탕으로 로그의 데이터를 가공 처리하여 모니터링DB를 구축한다.

## 공통 로그에 대한 키 및 값을 나열하고 각각에 대한 내용을 설명한다.

## 상호 다른 서비스에 대한 사용자 식별 및 추적을 위해 공통 필드를 기술한다.

## 로그 보존기간에 대한 정책이 존재해야 하며 이에 대한 프로세스 구성을 통해서 로그보존기간에 맞는 로그 운영이 필요하다.

1. **서비스 로그 개요**

## 기능

## 로그가 제공하는 기능은 다음과 같다.

|  |  |  |
| --- | --- | --- |
| NO | 기능 | 설명 |
| 1 | 추적 | * 서비스 프로세스는 각 프로세스의 로그를 각자의 로그파일에 접속되는 SESSION에 대한 정보를 단계별로 기록한다. * 로그 기록시 SESSION에 대한 Unique ID를 제공하며 이 값을 판단으로 SESSION에 대한 추적을 할 수 있다. |
| 2 | 에러 판단 | * 추적 기능과 더불어 SESSION에서 에러가 발생시 어떤 이유로 에러가 발생 했는가에 대한 정보가 로그에 기록된다. |
| 3 | 실시간  모니터링 | * 각 서버에서 제공되는 로그는 메시지에 대한 실시간 정보를 위해 특정 키워드를 제공한다. * 모니터링 프로세스는 이 키워드를 바탕으로 DB로 구성될 데이터를 가공하여 관리한다. |
| 4 | 통계 | * 실시간 로그를 바탕으로 통계 프로세스는 알맞게 재 구성하여 통계 데이터로 구축한다. |
| 5 | Syslog (옵션) | * Syslogd 를 통해 프로세스 사이에서 발생되는 로그정보를 설정된 SYSLOG로 보낼 수 있다. * Syslogd로 출력하기 위해 /etc/syslog.conf 에서 기능에 맞게 로그 파일 이름을 설정합니다. |
| 6 | 로그의  단계/종류 구분 | * 로그 단계를 설정하여 우선순위에 맞게 로그가 기록될 수 있다. * 관리자가 디버그 및 SYS로그에 대한 on/off 스위치를 제공하여 꼭 필요한 로그만을 기록할 수 있게 되어 있다. |
| 7 | 개발자용 디버깅 정보 | * 개발자가 필요로 하는 당시 상황에 대한 환경 정보가 기록된다. * 개발자가 알 수 있는 소스코드에 대한 정보도 기록된다. |

## 분류

## 프로세스 처리 로그

## Web Access 로그

## 로그 파일

## 로그 출력 기본 설정

|  |  |  |
| --- | --- | --- |
| NO | 구성 | 내용 |
| 1 | 기본 디렉터리 | 설정을 통해 로그 출력 경로를 지정할 수 있도록 해야 하며 각 서비스에 따라 경로를 일원화 할 수 있도록 한다.  {어플리케이션 로그 Home}은 가변 영역으로 서비스에 따라 달라질 수 있다. 단, 스템적으로 통일할 수 있다면 해당 디렉토리를 /logdata/, /weblog/ 형태로 고정할 수 있도록 한다. |
| 2 | 프로세스 구분 | {어플리케이션 로그 home}/PROCESS\_NAME 형태로 디렉토리를 구분한다. . |
| 3 | 파일 이름 | PROCESS\_NAME디렉터리 하위에 YYYYMMDD.log형식으로 기록한다 |
| 4 | Aging 설정 | 보존기간을 설정하고 자동으로 로그가 삭제될 수 있도록 한다.  로그의 보존기간은 각 서비스 및 로그데이터의 종류에 따라 보존기간이 상이할 수 있다.  자동삭제 방식은 어플리케이션에서 수행하도록 설정을 하는 것을 기본으로 하되 그렇지 못하는 경우는 배치잡을 설정하여 삭제할 수 있도록 한다. 서비스 배포시에 이에 대한 로그 보존기간에 따른 자동 삭제 프로세스를 검토하여 기능 누락이 되지 않도록 한다. |
| 5 | 압축 설정 (옵션) | 특정 기간이 지난 로그는 압축을 하여 보관 하도록 한다.  통상 3일이 지난 로그를 압축하도록 한다. |

## 로그 기본 보관기간 : 30일 기준

## 로그 기본기간을 넘겨서 보관해야 하는 경우 별도 로그서버를 통해서 보관하거나 필요로그만을 별도 추출하여 로그를 보관하는 방법을 취하도록 한다.

## 로그 LEVEL or 심각도 (Severity)

## 로그는 기록시 level과 종류를 정해 기록하고 있다.

## 로그는 중요도에 따라 선택적으로 표현되며 아래와 같이 5가지로 구분된다.

|  |  |  |
| --- | --- | --- |
| 중요도 | 종류 | 상 황 |
| 5 | ERROR | 비정상적인 상황  어플리케이션의 중요한 기능이 실패한 경우  자체 복구 불가능  바로 조치가 필요함. |
| 4 | WARN | 비정상적인 상황  자체 복구 가능  빠른 시일 내에 오작동을 수정 필요 |
| 3 | INFO | 정상적인 상황  개발 / 운영에 도움이 되는 정보 |
| 2 | DEBUG | 디버깅시 필요한 정보 |
| 1 | TRACE | 디버깅시 필요한 정보 |

참고) 로그레벨의 예제

*Logback :*

*ERROR > WARN > INFO > DEBUG > TRACE*

*Syslog :*

*Emergency > Alert > Critical > Error > Warning > Notice > Information > Debug*

* 서비스에 따라 적절한 로그레벨을 사용하도록 하고 가능하면 Log Library에서 제공하는 로그레벨을 사용

1. **프로세스 로그 - 필드 및 내용**

## 제약조건

## 실시간 모니터링 및 통계에 사용되는 로그에 대해서만 해당 필드 및 내용이 적용 된다.

## 관련 프로세스 : 업무 처리 프로세스

## 별도 수집이 필요한 로그에는 별도 수집을 위한 로그라는 마크를 구분하여 처리하는 방식을 검토한다. 해당 마크를 표기하는 방식은 향후 검토 예정입니다. %msg 출력에 포함 합니다. (옵션)

## 공통사항 값이 없는 경우 원활한 파싱을 위해서 “-“으로 표시도록 합니다.

|  |  |
| --- | --- |
| 종류 | 예 |
| 로그 샘플 | 2024-07-01 00:02:16.324 DO 8e51aeb7-eb5b-49c7-a9a9-efbe1ac5e66b \*\*\*\*\*\*\*\*@ktcloud.com [http-nio-80-exec-278] WARN c.d.g.a.h.dc.KtcAgreementBoxSetter - no matching agreement group found in html. |
| 로그 포맷 | %d{yyyy-MM-dd’T’HH:mm:ss.SSSZ} DO %X{session.id} %X{attr.email} [%thread] %-5level %logger{36}[%method:%line] - %msg%n |

## 필드

## 필수 데이터가 존재하고 각 필드의 연관 관계에 따라 표현 여부가 결정된다.

* + - * + Java logback 라이브러리 기준

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 | 설명 | 필수  사항 | 내용 |
| Date | 날짜 형식  1) 국제 표준  %d{yyyy-MM-dd’T’ HH:mm:ss.SSSZ}  Or  2) 일반적 표준  %d{yyyy-MM-dd HH:mm:ss.SSS} | O | 처리 날짜 및 시간 출력 (millisecond 단위는 옵션)  2024-07-01T10:44:11.020+0900  Or  2024-07-01 10:44:11.020  권장은 1)번이나 2)번도 가능  +0900 : 타임존 표기는 선택사항 |
| level | 로그 레벨  $-5level | O | 로그 레벨 또는 심각도를 출력  Logback 기준 참조 |
| 서비스 식별자 | 케이티클라우드에서 제공하는 서비스를 식별하기 위한 코드  Ex) KTC  \* 대문자로 출력 | O | 아래와 같은 코드로 서비스를 구분 / 케이티클라우드에서 제공하는 서비스를 식별할 수 있도록 기준 관리 필요  코드 생성/수정/삭제등에 대해서는 보안팀 / 운영팀에서 협의 결정    문자매니아  : SM   비즈메일러 : BM |
| 세션 식별자 | 처리 세션 식별자  Ex) %X{session.id} | X | 처리 프로세스를 식별할 수 있는 정보  8e51aeb7-eb5b-49c7-a9a9-efbe1ac5e66b |
| 사용자 식별자 | 사용자를 식별할 수 있는 정보  Ex) %X{attr.email} | X | \*\*\*\*\*\*\*\*@ktc.com  Ex) Id 또는 Email 정보  배치 프로세스등의 경우 사용자 식별정보가 없을 수 있어 필수값으로 표시 하지 않습니다.  값이 없는 경우 “-“ 표시가 되도록 합니다. |
| thread | 처리 스레드 식별자  [%thread] | O | [http-nio-8080-exec-5] |
| logger | 로그 출력 클래스  Ex) logger{36} | O | 로그를 출력하는 실제 클래스 출력 |
| method | 메소드 출력  [%method:%line] | X | lambda$getOrder$2 |
| line | 로그 출력 라인  [%method:%line] | X | 로그 출력 라인 : 92 |
| msg | 출력 메시지 | O | 처리 프로세스의 메시지를 출력  msg안에는 서비스에 맞는 형식을 고려  형식은 기계적으로 파싱을 할 수 있는 형식을 고려 |

1. **웹 억세스 로그 - 필드 및 내용**

## Access 로그 샘플 및 포맷

## 실시간 모니터링 및 통계에 사용되는 로그에 대해서만 해당 필드 및 내용이 적용 된다.

## 관련 프로세스 : 웹 억세스 로그 프로세스 (Apache / Nginx등)

## 샘플은 필드 설명의 권장사항을 참조하여 진행하도록 한다.

|  |  |
| --- | --- |
| 종류 | 예 |
| 로그 샘플 | 10.148.230.130 KTC http-nio-80-exec-337 \*\*\*\*\*@ktc.com [15/Sep/2024:00:00:00 +0900] GET /api/info HTTP/1.1 200 539 "https://ktc.com/app/home" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36" "" 0.134 |
| 로그 포맷 샘플 | %{X-Forwarded-For}i DO %I %{email}r [%{yyyy-MM-dd’T’HH:mm:ss.SSSZ}t] %r %s %b &quot;%{Referer}i&quot; &quot;%{User-Agent}i&quot; &quot;%{GO-Agent}i&quot; %T |

## 필드

## 필수 데이터가 존재하고 각 필드의 연관 관계에 따라 표현 여부가 결정된다.

* + - * + Apache Access로그 형식 기준

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 | 설명 | 필수  사항 | 내용 |
| 접속 IP | %{X-forwarded-For}  Or  %i | O | 프록시 또는 Load balancer IP  Or  Remote address  X-Forwarded-For IP가 없으면 실제 접속 아이피 출력  10.148.230.130 |
| 서비스 식별자 | 다우기술에서 제공하는 서비스를 식별하기 위한 코드 | X | 아래와 같은 코드로 서비스를 구분 / 다우기술에서 제공하는 서비스를 식별할 수 있도록 기준 관리 필요 / 대문자 출력  코드 생성/수정/삭제등에 대해서는 보안팀 / 운영팀에서 협의 결정  문자매니아  : SM   비즈메일러 : BM |
| 처리식별자 | 처리 쓰레드 식별자  %I | O | 처리 쓰레드 식별자  http-nio-80-exec-337 |
| 사용자 식별자 | 사용자를 식별할 수 있는 정보  %X{attr.email} | O | \*\*\*\*\*@ktc.co.kr  Ex) Id 또는 Email 정보 |
| 처리시간 | 날짜 형식 출력   1. 일반 표기   [%{yyyy-MM-dd HH:mm:ss.SSS}t]  Or   1. 국제표준 표기   [%{yyyy-MM-dd’T’HH:mm:ss.SSSZ}t] | O | 처리 날짜 출력  [2024-07-01 09:15:11.234]  Or  [2024-07-01T09:15:11.234+0900]  가급적 millisecond 로 표기를 하도록 권장하고 2) 국제 표준 표기를 권장한다.  타임존 표기는 선택사항 |
| Request 정보 | 요청 정보 출력  %r | O | 요청 처리 방식 / URL / HTTP 프로토콜  "GET /api/board/ HTTP/1.1" |
| 서버 응답코드 | 서버 처리 응답 코드  %s | O | 서버 응답 코드  200 |
| Byte Sent | 서버 응답 크기  %b | O | 서버 처리 byte 수  539 |
| Referer | Referrer URL  &quot;%{Referer}i&quot; | O | 호출 요청이 들어온 페이지 (referer URL)  "https://ktc.co.kr/app/home” |
| User-Agent | 사용자가 사용하는 Agent의 종류를 출력  &quot;%{User-Agent}i&quot; | O | 사용자 브라우저 종류 등을 출력  반드시 “ 로 묶어서 표현  "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36" |
| 추가 정보 | 예)  &quot;%{GO-Agent}i&quot; | X | 헤더의 특정 정보등을 출력 |
| 처리시간 | 해당 처리를 수행하는데 소요된 시간  %T | O | 성능 및 개선점을 찾기 위한 처리시간 출력  0.134 – 단위 : 초 (소수점 3자리까지 출력) |

* 추가 정보를 출력하는 경우 User-Agent와 처리시간 사이에 넣도록 한다.

## 적용범위

* 현재 운영중인 서비스 및 향후 개발센터에서 개발되는 모든 프로세스가 대상
* PHP및 C데몬의 프로세스 로그의 경우 상기 로그 형식과 차이가 있어 추가 검토를 수행하고 별도 기준을 마련하도록 한다.

## 필수사항

* 적용 범위와 무관하게 로그 출력은 기본적으로 로그 라이브러리를 통해서 출력이 되도록 해야 하며 그 로그 출력 기준이 되는 라이브러리의 선택은 각 서비스 플랫폼별로 공통으로 사용할 수 있도록 고려한다.