# 시스로그 설비 및 우선순위 참조표

## 개요

시스로그(Syslog)는 네트워크 장비와 시스템에서 로그 메시지를 전송하는 표준 프로토콜입니다. 각 시스로그 메시지는 **Facility**(설비)와 **Severity**(심각도)의 조합으로 우선순위를 나타내며, 이는 **PRI 상수값**으로 계산됩니다.

## PRI 상수값 계산 방법

PRI 상수값은 다음 공식으로 계산됩니다:

PRI = Facility × 8 + Severity

### 계산 예시

* **Facility**: 16 (local0)
* **Severity**: 6 (info)
* **PRI 상수값**: 16 × 8 + 6 = 134

## Facility (설비) 코드

|  |  |  |
| --- | --- | --- |
| 코드 | 설비명 | 설명 |
| 0 | kern | 커널 메시지 |
| 1 | user | 사용자 레벨 메시지 |
| 2 | mail | 메일 시스템 |
| 3 | daemon | 시스템 데몬 |
| 4 | auth | 보안/인증 메시지 |
| 5 | syslog | 시스로그 데몬에서 내부적으로 생성 |
| 6 | lpr | 라인 프린터 서브시스템 |
| 7 | news | 네트워크 뉴스 서브시스템 |
| 8 | uucp | UUCP 서브시스템 |
| 9 | clock | 클럭 데몬 |
| 10 | authpriv | 보안/인증 메시지 |
| 11 | ftp | FTP 데몬 |
| 12 | ntp | NTP 서브시스템 |
| 13 | audit | 로그 감사 |
| 14 | alert | 로그 알람 |
| 15 | solaris-cron | 클럭 데몬 (Solaris) |
| 16 | local0 | 로컬 사용 설비 0 |
| 17 | local1 | 로컬 사용 설비 1 |
| 18 | local2 | 로컬 사용 설비 2 |
| 19 | local3 | 로컬 사용 설비 3 |
| 20 | local4 | 로컬 사용 설비 4 |
| 21 | local5 | 로컬 사용 설비 5 |
| 22 | local6 | 로컬 사용 설비 6 |
| 23 | local7 | 로컬 사용 설비 7 |

## Severity (심각도) 코드

|  |  |  |
| --- | --- | --- |
| 코드 | 심각도명 | 설명 |
| 0 | emerg | Emergency: 시스템이 사용할 수 없음 |
| 1 | alert | Alert: 즉시 조치가 필요함 |
| 2 | crit | Critical: 심각한 상태 |
| 3 | error | Error: 오류 상태 |
| 4 | warn | Warning: 경고 상태 |
| 5 | notice | Notice: 정상이지만 중요한 상태 |
| 6 | info | Informational: 정보성 메시지 |
| 7 | debug | Debug: 디버그 레벨 메시지 |

## PRI 상수값 참조표

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Facility(↓)<br />Severity(→) | 0/Emer | 1/Alert | 2/Crit | 3/Error | 4/Warn | 5/Notice | 6/Info | 7/Debug |
| 0 / kern | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 / user | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 / mail | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 3 / deamon | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 4 / auth | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 5 / syslog | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| 6 / lpr | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 |
| 7 / news | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| 8 / uucp | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| 9 / clock | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| 10 / authpriv | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 |
| 11 / ftp | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 |
| 12 / ntp | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 |
| 13 / audit | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 |
| 14 / alert | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 |
| 15 / solaris-cron | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 |
| 16 / local0 | 128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 |
| 17 / local1 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 |
| 18 / local2 | 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 |
| 19 / local3 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 |
| 20 / local4 | 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 |
| 21 / local5 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 |
| 22 / local6 | 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 |
| 23 / local7 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 |

## 사용 방법

### 로그프레소 소나에서 사용하기

시스로그 수집기 설정에서 **시스로그 설비 목록** 필드에 원하는 PRI 상수값을 입력합니다:

* **단일 값**: 134 (local0.info)
* **여러 값**: 134,135,136 (local0의 info, debug, local1의 emerg)
* **모든 값**: 비워두세요.

### 특수 값

* **빈 값**: 모든 facility 값을 입력한 것과 같음 (모든 메시지 수집)

## 참고 자료

* [RFC 5424 - The Syslog Protocol](https://tools.ietf.org/html/rfc5424)
* [RFC 3164 - The BSD Syslog Protocol](https://tools.ietf.org/html/rfc3164)