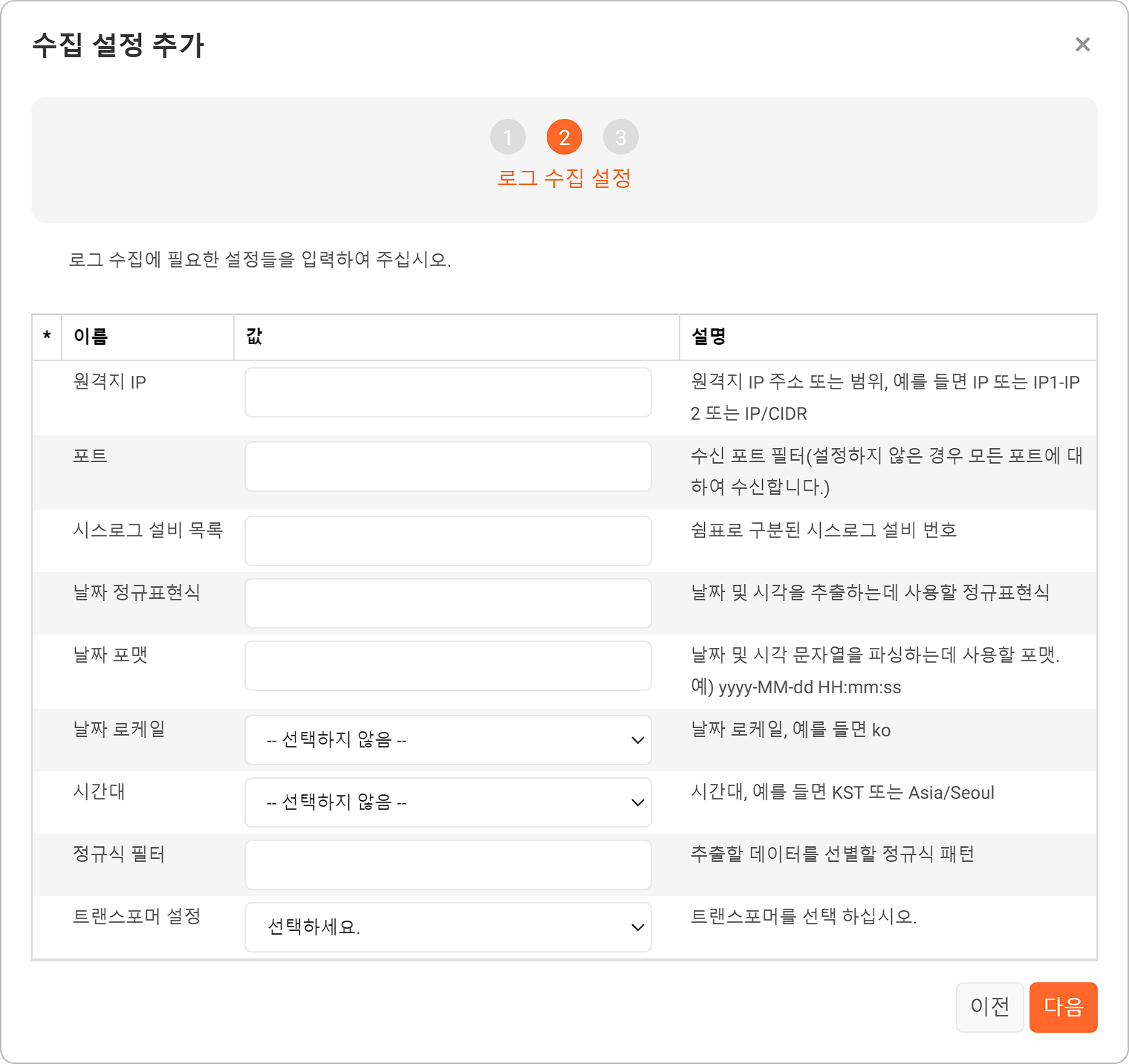
#### 시스로그

시스로그 로거는 원격 호스트가 전송하는 Syslog 메시지를 수신합니다.



시스로그

시스로그 로거는 **시스템 > 포트 관리**에서 구성한 시스로그 포트를 통해 실시간으로 TCP 및 UDP 시스로그를 수집합니다.



**원격지 IP**

시스로그 로거가 메시지를 수신할 원격지 IP 주소 또는 주소 대역. 입력값은 단일 IP 주소(예: 192.168.0.1), 시작 주소와 끝 주소 사이에 하이픈(-)이 있는 IP 주소 범위(예: 192.168.0.1-192.168.0.254), CIDR 표기법에 따른 IP 주소 대역(예: 192.168.0.0/24) 형식으로 사용해야 합니다.

**시스로그 설비 목록**

[RFC 5424](https://tools.ietf.org/html/rfc5424)에 정의된 PRI 상수값. 여러 개의 PRI 상수를 지정하려면 구분자로 쉼표(,)를 이용합니다. PRI 상수값을 지정하지 않으려면 -1을 입력합니다. 모든 시스로그를 수신하려면 RFC 5424에 나온대로 -1부터 23까지 모두 입력하십시오. 아무 값도 입력하지 않으면 모든 facility 값을 입력한 것과 같습니다.

PRI 상수값은 Facility 값의 8배수에 Severity 값을 더한 값입니다. 다음 표를 참조해서 계산된 값을 사용하십시오.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

**날짜 정규표현식**

시스로그에서 날짜 및 시각을 추출하는데 사용할 정규표현식

**날짜 포맷**

날짜 문자열을 파싱하는데 사용할 날짜 포맷(예: yyyy-MMM-dd HH:mm:ss). 날짜 로케일에 따라 파싱하는 형식이 다를 수 있습니다.

**날짜 로케일**

날짜 문자열의 로케일(기본값: en). 가령 날짜 파싱 포맷 지시자 중에서 MMM은 로케일에 따라 **Jan**(로케일이 en일 때) 혹은 **1월**(로케일이 ko일 때)로 해석됩니다.

**시간대**

시간대를 목록에서 선택. API를 이용해 로거를 구성하는 경우 KST 또는 Asia/Seoul와 같은 형식으로 시간대를 지정할 수 있습니다.

**정규식 필터**

추출할 데이터를 선별할 정규식 패턴을 입력합니다.

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.