Juniper SRX 日本語マニュアル

System Logging の CLI 設定

JUNIPER NETWORKS | Driven by Experience™

はじめに

- 本マニュアルは、System Logging の CLI 設定について説明します
- 手順内容は SRX300 、Junos 21.2R3-S2 にて確認を実施しております
- 実際の設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  https://www.juniper.net/documentation/

- 他にも多数の SRX 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/security.html

2022 年 8 月

System Logging

以下の設定を行う場合のコマンド例となります

- SRX 上の messages ファイルに保存
  Facility : any
  Severity Level : error

- Syslog サーバ (192.30.80.76) に送信
  Facility : any
  Severity Level : any

- デフォルトの設定は下記となります

```
user@srx> show configuration system syslog | display set
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
```

System Logging

1. SRX 上の messages ファイルに保存します

```
user@srx# set system syslog file messages any error
```

2. Syslog サーバに Syslog を送信します

```
user@srx# set system syslog host 192.30.80.76 any any
```

System Logging

設定の確認

```
user@srx# show
    syslog {
        host 192.30.80.76 {
            any any;
        }
        file messages {
            any error;
        }
    }
}
```

System Logging

messages ファイルのログ確認

```
user@srx> show log messages
Apr 22 02:33:22  srx mgd[2405]: UI_CMDLINE_READ_LINE: User 'user', command 'configure '
Apr 22 02:33:22  srx mgd[2405]: UI_DBASE_LOGIN_EVENT: User 'user' entering configuration mode
Apr 22 02:33:24  srx mgd[2405]: UI_CMDLINE_READ_LINE: User 'user', command 'exit '
Apr 22 02:33:24  srx mgd[2405]: UI_DBASE_LOGOUT_EVENT: User 'user' exiting configuration mode
Apr 22 02:33:32  srx mgd[2405]: UI_CMDLINE_READ_LINE: User 'user', command 'show log messages '
...（以下省略）
```

System Logging

ヘルプの確認

```
user@srx> help syslog
Syslog tag                          Help
AAMW_ACTION_LOG                     AAMW action info
AAMW_ACTION_LOG_LS                  AAMW action info
AAMW_CONTENT_FALLBACK_LOG           AAMW content fallback info
AAMW_CONTENT_FALLBACK_LOG_LS        AAMW content fallback info
AAMW_HOST_INFECTED_EVENT_LOG        AAMW cloud event host infected info
AAMW_HOST_INFECTED_EVENT_LOG_LS     AAMW cloud event host infected info
AAMW_IMAP_ACTION_LOG                AAMW IMAP action info
AAMW_IMAP_ACTION_LOG_LS             AAMW IMAP action info
AAMW_MALWARE_EVENT_LOG              AAMW cloud event malware detected info
AAMW_MALWARE_EVENT_LOG_LS           AAMW cloud event malware detected info
...（以下省略）
```

ヘルプの詳細内容確認

```
user@srx> help syslog UI_LOGIN_EVENT
Name:          UI_LOGIN_EVENT
Message:       User '<username>' login, class '<class-name>'
               <local-peer>[<pid>], ssh-connection '<ssh-connection>',
               client-mode '<client-mode>'
Help:          User started CLI session
Description:   The indicated user started a Junos OS CLI session.
Type:          Event: This message reports an event, not an error
Severity:      info
Facility:      ANY
```


Thank you
JUNIPER NETWORKS
Driven by Experience™