



製品ガイド

Syslog Watcher 4

平成23年4月27日



ジュピターテクノロジー



製品概要

Syslog Watcherは米国SNMPSOFT社が開発したWindows環境のSyslogソリューションです。

2011年1月にはVer 4がリリースされました。

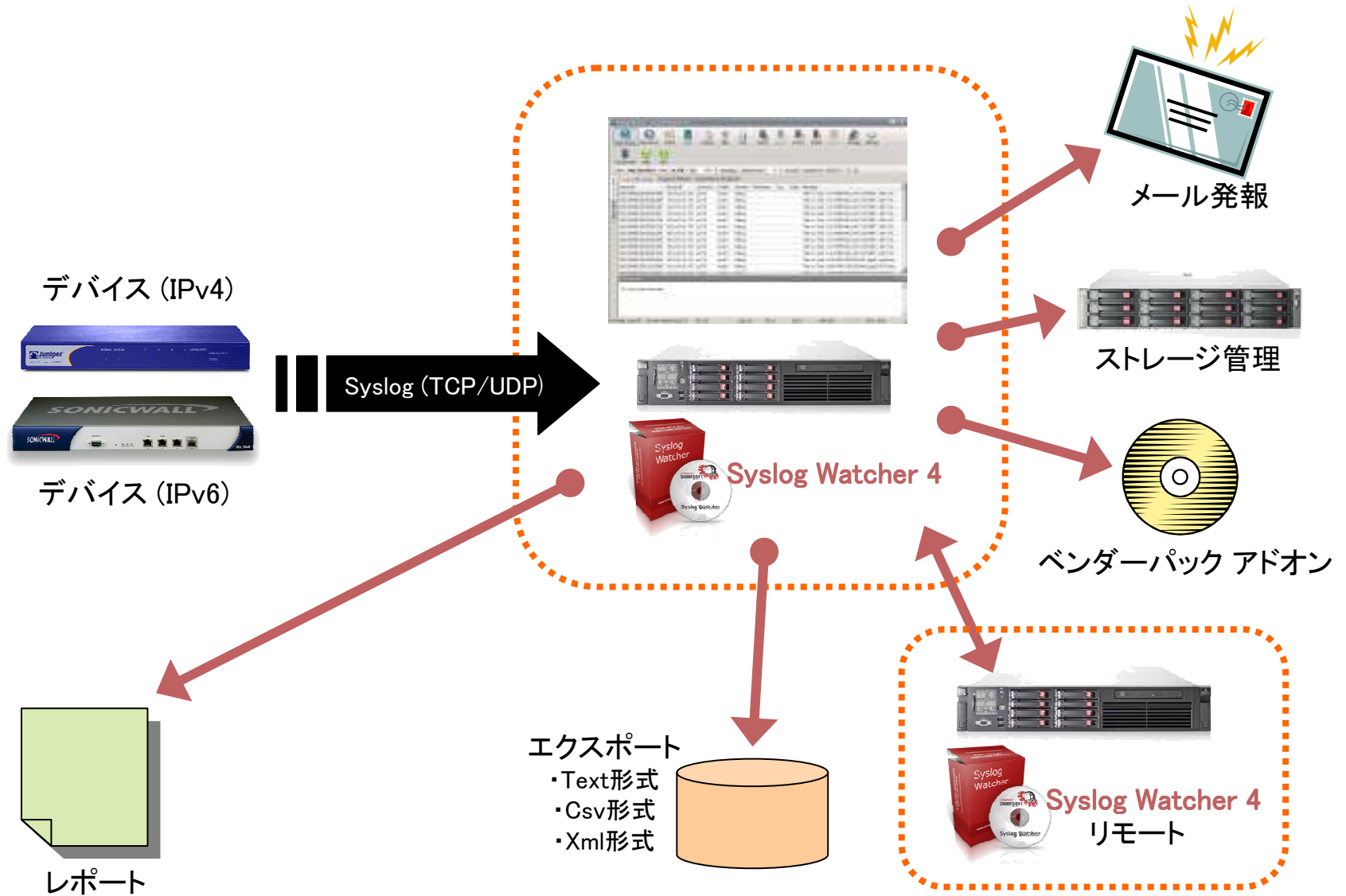
Syslog格納用にカスタマイズされた特殊なデータベースを用いるため作業レスポンスが非常に軽いのが特徴で、3千メッセージ/秒の受信が可能、かつ1万4千種類以上のSyslogを解釈可能であり、IPv4/IPv6に正式対応をしています。

また、リモートで別のSyslog Watcherを参照することが可能です。





ログ処理イメージ





システム要件

◆ハードウェア最小要件

CPU	: 1GHz
メインメモリ	: 512MB
HDD容量	: 50MB + data
その他	: Network Interface



◆ソフトウェア要件

OS	: Windows 2000/XP/2003(32bit・64bit) 2008(32bit・64bit)/Vista(32bit・64bit) 7(32bit・64bit)
----	---



メイン・インターフェース

最新のログ取り込みの時間間隔を調整できます。

The screenshot displays the Syslog Watcher application window. The main area shows a table of log messages with columns for Received, Source IP, Source Name, Facility, Severity, Timestamp, Text, Origin, and Message. The messages are sorted by timestamp, showing various events from 2011/04/05. A 'Message View' section at the bottom provides a detailed look at a selected message: 'Notice / local1: logawa_pc [192.168.10.14] Test user connected to website http://205.71.41.42/index.html'.

Received	Source IP	Source Name	Facility	Severity	Timestamp	Text	Origin	Message
2011/04/05 11:32:27.218	192.168.10.14	logawa_pc	local1	Warning				Test user connected to website http://200.15.241.83/index.html
2011/04/05 11:32:27.000	192.168.10.14	logawa_pc	local1	Debug				Test user connected to website http://206.219.200.95/index.html
2011/04/05 11:32:26.750	192.168.10.14	logawa_pc	local1	Emergency				Test user connected to website http://199.193.207.180/index.html
2011/04/05 11:32:22.562	192.168.10.14	logawa_pc	local1	Info				This is a test message generated by Kivi SyslogGen
2011/04/05 11:32:22.328	192.168.10.14	logawa_pc	local1	Critical				This is a test message generated by Kivi SyslogGen
2011/04/05 11:32:21.761	192.168.10.14	logawa_pc	local1	Critical				This is a test message generated by Kivi SyslogGen
2011/04/05 11:32:21.609	192.168.10.14	logawa_pc	local1	Warning				This is a test message generated by Kivi SyslogGen
2011/04/05 11:32:04.125	192.168.10.14	logawa_pc	local1	Warning				Good morning!
2011/04/05 11:32:01.765	192.168.10.14	logawa_pc	local1	Notice				Good night!
2011/04/05 11:31:28.421	192.168.10.14	logawa_pc	local1	Notice				Error reading from specified file
2011/04/05 11:31:22.250	192.168.10.14	logawa_pc	local1	Info				This is a test message generated by Kivi SyslogGen
2011/04/05 11:31:22.046	192.168.10.14	logawa_pc	local1	Info				This is a test message generated by Kivi SyslogGen
2011/04/05 11:31:21.795	192.168.10.14	logawa_pc	local1	Emergency				This is a test message generated by Kivi SyslogGen
2011/04/05 11:31:21.562	192.168.10.14	logawa_pc	local1	Info				This is a test message generated by Kivi SyslogGen
2011/04/05 11:30:08.062	192.168.10.14	logawa_pc	local1	Critical				The quick brown fox jumps over the lazy dog.
2011/04/05 11:30:06.421	192.168.10.14	logawa_pc	local1	Critical				The quick brown fox jumps over the lazy dog.
2011/04/05 11:30:05.750	192.168.10.14	logawa_pc	local1	Warning				The quick brown fox jumps over the lazy dog.
2011/04/05 11:30:04.140	192.168.10.14	logawa_pc	local1	Warning				The quick brown fox jumps over the lazy dog.
2011/04/05 11:29:54.609	192.168.10.14	logawa_pc	local1	Notice				The quick brown fox jumps over the lazy dog.
2011/04/05 11:29:15.500	192.168.10.14	logawa_pc	local1	Error				Error reading from specified file
2011/04/05 11:29:09.718	192.168.10.14	logawa_pc	local1	Info				This is Syslog test message number 3
2011/04/05 11:29:09.468	192.168.10.14	logawa_pc	local1	Critical				This is Syslog test message number 2
2011/04/05 11:29:00.921	192.168.10.14	logawa_pc	local1	Debug				This is Syslog test message number 1
2011/04/05 11:28:52.062	192.168.10.14	logawa_pc	local1	Error				Test user connected to website http://199.48.148.21/index.html
2011/04/05 11:28:51.812	192.168.10.14	logawa_pc	local1	Notice				Test user connected to website http://206.105.181.88/index.html
2011/04/05 11:28:51.484	192.168.10.14	logawa_pc	local1	Notice				Test user connected to website http://205.71.41.42/index.html



Syslog Watcherの動作モード

1. Standalone Application
サーバ上で単体のアプリケーションとして動作します
2. Local Syslog Server
ローカルサーバ上でWindowsのサービスとして動作します
3. Remote Server
別のサーバ上のSyslog Watcherをリモートで監視します



Standalone Applicationモードについて

The screenshot displays the Syslog Watcher - Local Syslog Server application window. The interface includes a menu bar with options like Start Server, Stop Server, Status, Reload, Filter, Find, Search, Import, Export, Delete, Reports, Storage, and Settings. Below the menu bar, there are buttons for Vendor Pack, Help, and Info. The main area shows a list of received syslog messages with columns for Received, Source IP, Source Name, Message, Facility, Severity, and T. T. O... The status bar at the bottom indicates Service: Started (4.2.2) Tot: 4,118, Dsp: 500, Flt: 0, Sel: 1, UDP: 514, TCP: 1468, IPv4, IPv6, Ver: 4.2.

Received	Source IP	Source Na...	Message	Facility	Severity	T. T. O...
2011/04/22 17:27:27.321	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	user-level	Warning	
2011/04/22 17:27:26.306	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	NTP	Info	
2011/04/22 17:27:25.293	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 6	Critical	
2011/04/22 17:27:24.278	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 4	Emergency	
2011/04/22 17:27:23.264	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	UUCP	Debug	
2011/04/22 17:27:22.250	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 4	Info	
2011/04/22 17:27:21.236	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	user-level	Error	
2011/04/22 17:27:20.221	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 3	Notice	
2011/04/22 17:27:19.209	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	kernel	Info	
2011/04/22 17:27:18.196	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	news	Info	
2011/04/22 17:27:17.183	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	log audit	Critical	
2011/04/22 17:27:16.174	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 0	Warning	

サーバ上で単体のアプリケーションとして動作するモードです。



Local Syslog Serverモードについて

The screenshot displays the Syslog Watcher - Local Syslog Server application window. The interface includes a menu bar with options like Start Server, Stop Server, Status, Reload, Filter, Find, Search, Import, Export, Delete, Reports, Storage, and Settings. Below the menu bar, there are buttons for Vendor Pack, Help, and Info. The main area shows a list of received syslog messages with columns for Received, Source IP, Source Name, Message, Facility, Severity, and T. T. O... The status bar at the bottom indicates the service is started, showing statistics like Dsp: 500, Flt: 0, Sel: 1, and supported protocols like UDP: 514, TCP: 1468, IPv4, IPv6, Ver: 4.2.

Received	Source IP	Source Na...	Message	Facility	Severity	T. T. O...
2011/04/22 17:27:27.321	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	user-level	Warning	
2011/04/22 17:27:26.306	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	NTP	Info	
2011/04/22 17:27:25.293	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 6	Critical	
2011/04/22 17:27:24.278	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 4	Emergency	
2011/04/22 17:27:23.264	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	UUCP	Debug	
2011/04/22 17:27:22.250	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 4	Info	
2011/04/22 17:27:21.236	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	user-level	Error	
2011/04/22 17:27:20.221	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 3	Notice	
2011/04/22 17:27:19.209	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	kernel	Info	
2011/04/22 17:27:18.196	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	news	Info	
2011/04/22 17:27:17.183	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	log audit	Critical	
2011/04/22 17:27:16.174	192.168.10.133	sakurai-PC	This is a test message generated by Kiwi SyslogGen	local 0	Warning	

ローカルサーバ上でWindowsのサービスとして動作するモードです。



Remote Serverモードについて

The screenshot shows the Syslog Watcher - Remote Syslog Server application interface. The main window displays a list of received syslog messages with columns for Received, Source IP, Source Name, Message, Facility, and Severity. A dialog box titled 'Connect to Remote Server' is overlaid on the interface, containing the following fields and options:

- Server: 192.168.10.130 (with a Ping button)
- Port: 4010 (with a dropdown arrow)
- Use secure connection
- Password: (with a text input field)
- Remember
- Buttons: Connect, Cancel

Received	Source IP	Source Na...	Message	Facility	Si
2011/04/22 16:58:57.062			Original Address=212.95.98.129 This is a test mes...	local 4	Er
2011/04/22 16:58:56.062			Original Address=200.221.224.200 This is a test m...	mail	Di
2011/04/22 16:58:55.062			st me...	syslogd	In
2011/04/22 16:58:54.062			st me...	UUCP	Er
2011/04/22 16:58:53.062			mess...	mail	Er
2011/04/22 16:58:52.062			t mes...	log alert	Er
2011/04/22 16:58:51.062			st me...	syslogd	Ni
2011/04/22 16:58:50.062			st me...	UUCP	Er
2011/04/22 16:58:49.062			mess...	FTP	In
2011/04/22 16:58:48.062			Original Address=199.117.100.200 This is a test m...	local 1	Er

別のサーバ上のSyslog Watcherに接続することができるモードです。
接続先のSyslog Watcherにはポート番号、パスワードを設定できます。



ログ受信に関して

1. サポートプロトコル
→TCP/UDP
2. 処理性能
→3,000件/秒以上



操作画面

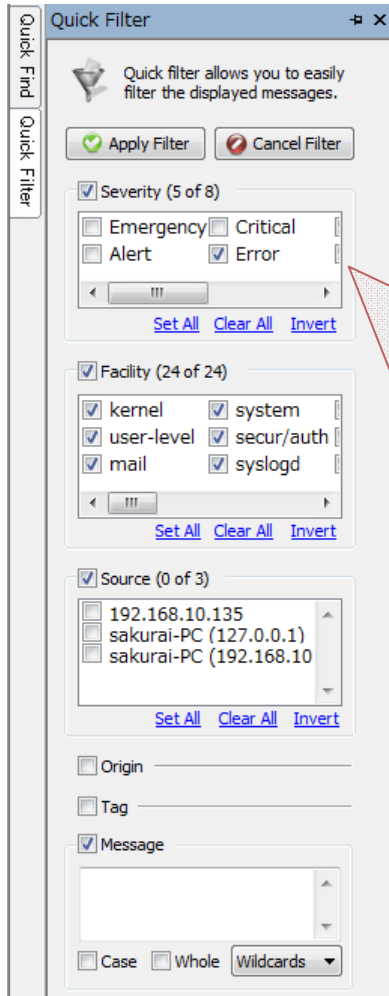
ネットワーク設定(受信ポート指定等)、Eメールによるアラート設定、日付フォーマット指定、リモートアクセス管理の許可・不許可などの設定ができます。

The screenshot displays the System Watcher application window. The main area shows a list of received syslog messages with columns for Received, Source IP, Source Name, Facility, Severity, Timestamp, Tot, Origin, and Message. An 'E-mail Alerts' dialog box is open, showing options for truncating large messages and a list of email alerts. The 'E-mail Alerts' list contains one entry: 'test1'. The dialog also includes fields for 'Email Subject...', 'Email Body...', and 'Recipient's e-mail address:'. The background shows the main interface with a toolbar and a status bar at the bottom.

Received	Source IP	Source Name	Facility	Severity	Timestamp	Tot	Origin	Message
2011/04/05 11:30:05.750	192.168.10.14	topaws_pc	local 1	Emergency				Test user connected to website http://192.168.207.180/index.html
2011/04/05 11:30:02.562	192.168.10.14	topaws_pc	local 1	Info				This is a test message generated by Kiwi SyslogGen
2011/04/05 11:30:02.308	192.168.10.14	topaws_pc	local 1	Critical				This is a test message generated by Kiwi SyslogGen
2011/04/05 11:30:01.761	192.168.10.14	topaws_pc	local 1	Critical				This is a test message generated by Kiwi SyslogGen
2011/04/05 11:30:01.608	192.168.10.14	topaws_pc	local 1	Warning				This is a test message generated by Kiwi SyslogGen
2011/04/05 11:30:04.125	192.168.10.14	topaws_pc	local 1	Warning				Good morning!
2011/04/05 11:30:01.765	192.168.10.14	topaws_pc	local 1	Notice				Good morning!



フィルター/検索/カラーリング



さまざまな条件によりシスログメッセージをフィルタリング/検索/カラーリングすることが可能です。

条件

Severity

シスログメッセージから抽出された重要度。

Facility

シスログメッセージから抽出されたファシリティ。

Tag

メッセージのタグ、メッセージにはソースに基づき目印が付きます。この情報はシスログメッセージ本文より抽出されます。またシスログのソースにより特定されます。更にサブシステムと一致、時として、連番メッセージになる事もあります。

Origin

追加情報、シスログメッセージ源。特定のシスログソース(例;メッセージのリアルソース名やアドレス)で、メッセージに追記することが可能です。

Message

シスログメッセージのテキスト内容。



フィルター例

The screenshot shows the 'Quick Filter' dialog box on the left and a table of log messages on the right. The dialog box has two sections: 'Severity (2 of 8)' and 'Facility (24 of 24)'. In the 'Severity' section, 'Emergency' and 'Critical' are checked, while 'Alert' and 'Error' are not. In the 'Facility' section, 'kernel', 'user-level', 'mail', 'system', 'secur/auth', and 'syslogd' are checked. The table on the right has columns for 'Source Name', 'Message', 'Facility', and 'Severity'. The messages are filtered to show only those with a severity of 'Critical' or 'Emergency'.

Source Name	Message	Facility	Severity
WIN-IRHXT0NDLLS	Original Address=209.3.206.21 This is ...	local 6	Critical
WIN-IRHXT0NDLLS	Original Address=212.78.236.116 This i...	clock (9)	Emergency
WIN-IRHXT0NDLLS	Original Address=206.71.28.236 This is...	syslogd	Emergency
WIN-IRHXT0NDLLS	Original Address=209.226.61.187 This i...	local 3	Critical
WIN-IRHXT0NDLLS	Original Address=202.233.99.214 This i...	user-le...	Emergency
WIN-IRHXT0NDLLS	Original Address=194.45.10.158 This is...	log audit	Emergency
WIN-IRHXT0NDLLS	Original Address=213.49.219.101 This i...	local 4	Critical
WIN-IRHXT0NDLLS	Original Address=207.48.154.249 This i...	local 0	Emergency
WIN-IRHXT0NDLLS	Original Address=216.101.86.53 This is...	syslogd	Critical
WIN-IRHXT0NDLLS	Original Address=196.147.68.221 This i...	syslogd	Emergency
WIN-IRHXT0NDLLS	Original Address=212.22.121.48 This is...	user-le...	Critical
WIN-IRHXT0NDLLS	Original Address=201.238.56.112 This i...	local 2	Critical
WIN-IRHXT0NDLLS	Original Address=211.99.103.95 This is...	mail	Emergency

Severityを条件としたフィルター例



検索例

Quick Find window showing search results. The search criteria are Facility (1 of 24) with FTP selected. The results table is as follows:

Source Name	Message	Facility	Severity
WIN-IRHXT0NDLLS	Original Address=209.226.128.196 This...	UUCP	Error
WIN-IRHXT0NDLLS	Original Address=216.7.56.99 This is a ...	local 4	Emergency
WIN-IRHXT0NDLLS	Original Address=201.80.61.204 This is...	local 3	Notice
WIN-IRHXT0NDLLS	Original Address=211.231.170.248 This...	FTP	Alert
WIN-IRHXT0NDLLS	Original Address=221.1.210.84 This is ...	log audit	Warning
WIN-IRHXT0NDLLS	Original Address=214.100.253.233 This...	system	Debug
WIN-IRHXT0NDLLS	Original Address=221.224.201.221 This...	local 5	Debug
WIN-IRHXT0NDLLS	Original Address=204.183.71.136 This i...	secur/...	Error
WIN-IRHXT0NDLLS	Original Address=200.176.61.38 This is...	secur/...	Critical
WIN-IRHXT0NDLLS	Original Address=193.146.72.17 This is...	secur/...	Debug
WIN-IRHXT0NDLLS	Original Address=220.12.163.206 This i...	mail	Info
WIN-IRHXT0NDLLS	Original Address=213.69.223.126 This i...	FTP	Critical
WIN-IRHXT0NDLLS	Original Address=216.193.216.97 This i...	user-le...	Alert

Facilityを条件とした検索例



カラーリング例

Received	Source IP	Sou...	Message	Facility	Severity	Ti...	Tag	Ori...
2011/04/20 15:00:05.890	192.168.10...	WIN...	Original Address=195.78.240.9 This is a...	local 6	Alert			
2011/04/20 15:00:04.890	192.168.10...	WIN...	Original Address=211.65.102.225 This i...	news	Alert			
2011/04/20 15:00:03.890	192.168.10...	WIN...	Original Address=219.85.66.32 This is a...	local 3	Critical			
2011/04/20 15:00:02.890	192.168.10...	WIN...	Original Address=207.131.65.164 This i...	news	Notice			
2011/04/20 15:00:01.890	192.168.10...	WIN...	Original Address=211.60.130.189 This i...	user-level	Warning			
2011/04/20 15:00:00.890	192.168.10...	WIN...	Original Address=203.116.230.133 This ...	FTP	Alert			
2011/04/20 14:59:59.890	192.168.10...	WIN...	Original Address=216.171.133.1 This is ...	clock (15)	Debug			
2011/04/20 14:59:58.890	192.168.10...	WIN...	Original Address=224.102.174.146 This ...	clock (9)	Error			
2011/04/20 14:59:57.890	192.168.10...	WIN...	Original Address=212.244.38.226 This i...	local 6	Error			
2011/04/20 14:59:56.890	192.168.10...	WIN...	Original Address=209.134.99.124 This i...	local 3	Debug			
2011/04/20 14:59:55.890	192.168.10...	WIN...	Original Address=224.198.45.153 This i...	clock (15)	Debug			
2011/04/20 14:59:54.890	192.168.10...	WIN...	Original Address=219.173.196.14 This i...	syslogd	Warning			
2011/04/20 14:59:53.890	192.168.10...	WIN...	Original Address=199.29.119.32 This is ...	system	Error			

Severityを条件としたカラーリング例



Eメールアラート機能

さまざまな条件によりアラートメールを送信することが可能です。

E-mail Alerts

Trim large syslog messages to: characters

List of e-mail alerts:

- New E-mail Alert

Criteria...
E-mail Subject...
E-mail Body...
Format: Text

Recipient's e-mail address:

Filter Criteria

Severity (8 of 8)

- Emergency
- Alert
- Critical
- Error

Facility (24 of 24)

- kernel
- user-level
- mail
- system

Source (0 of 3)

- 192.168.10.135
- sakurai-PC (127.0.0.1)
- sakurai-PC (192.168.10.133)

Origin (one per line)

設定可能条件

Severity
Facility
Tag
Origin
Message

Email Alert Body

Tag

```
<table cellpadding="3" class="frame s5ev-%SEVERITY_NUM%" style="width: 100%">
<tr>
<td class="style1">%SEVERITY% / %FACILITY%</td>
<td class="style1">%SOURCE_NAME% (%SOURCE_IP%)</td>
<td style="width: 30%">&nbsp;&nbsp;&nbsp;&nbsp;</td>
<td class="style2" style="text-align: right">%DATE_LONG% %TIME_LONG%</td>
</tr>
</table>
<div id="yp">%VENDOR_PACK%</div>
<div id="msg"><p>%MESSAGE%</p></div>
```

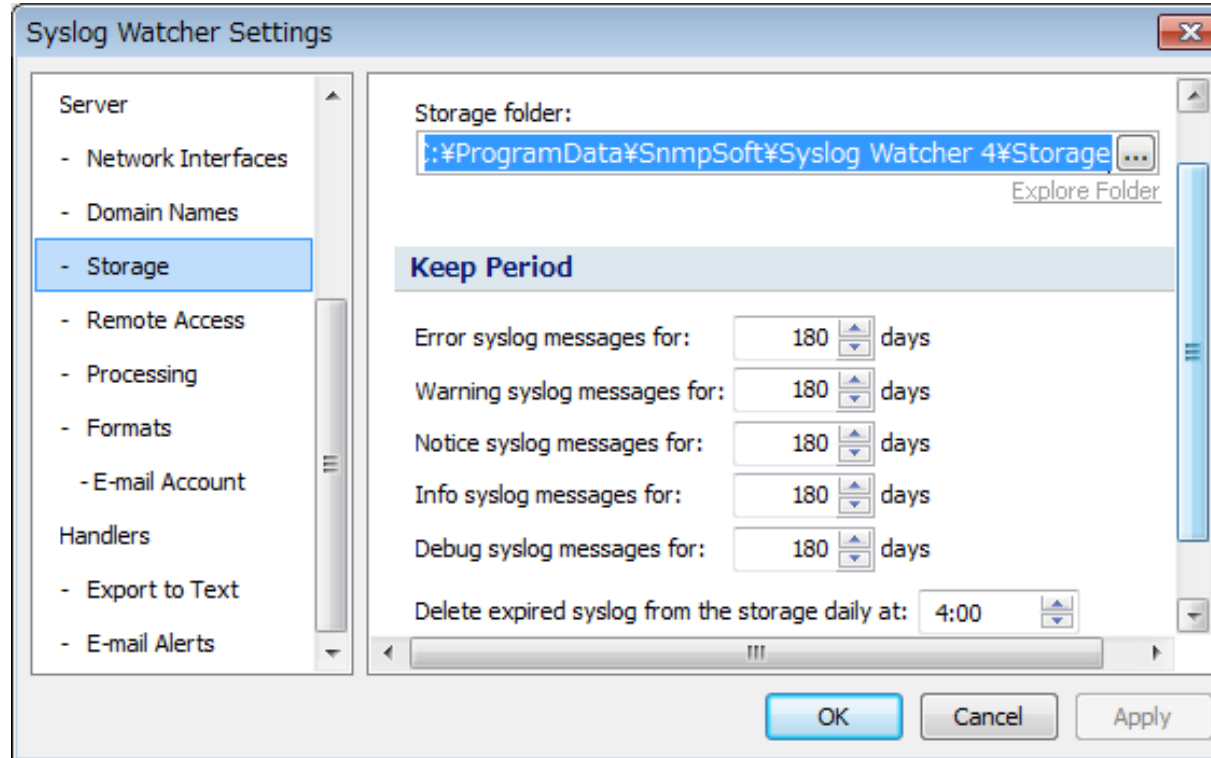
OK Cancel

1/04/04 10:26:01.630	192.168.10.133	sakura	%SEVERITY%
1/04/04 10:26:00.626	192.168.10.133	sakura	%FACILITY%
1/04/04 10:25:59.611	192.168.10.133	sakura	%ALERT_NAME%



シスログストレージ①

シスログメッセージは、Severityごとに保存期間を指定できます。



ストレージの圧縮も可能です。



シスログストレージ②

シスログストレージの状況はグラフィカルに確認できます。

- メッセージ数
- ストレージサイズ
- フリースペース

Syslog Storage Info
C:\ProgramData\Snmsoft\Syslog Watcher 4\Storage

Messages:	145
Storage size:	72,704
Free space:	105,510,576,128

Compact Clear Storage

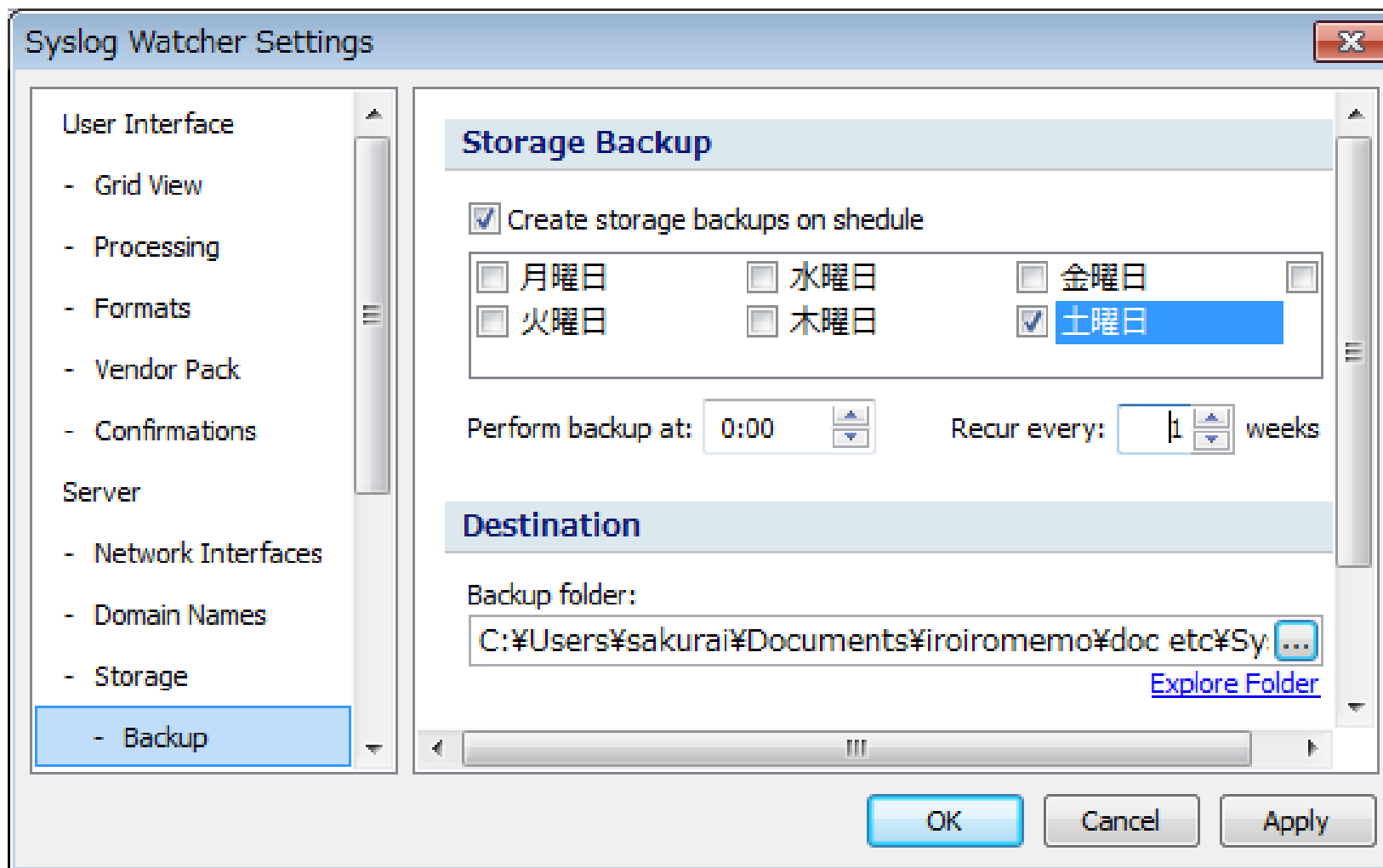
Bank	Size (bytes)	Messages	Last message
Errors	15,360	39	13 days 23 hours 6 minutes 41 secon...
Warnings	13,312	21	13 days 23 hours 6 minutes 42 secon...
Notices	8,192	11	14 days 3 hours 50 minutes 5 second...
Info	16,384	47	13 days 20 hours 1 minute 11 second...
Debug	12,288	27	14 days 3 hours 50 minutes 6 second...

火曜日, 3月 29, 2011 - 月曜日, 4月 04, 2011 (7 days)

Refresh OK



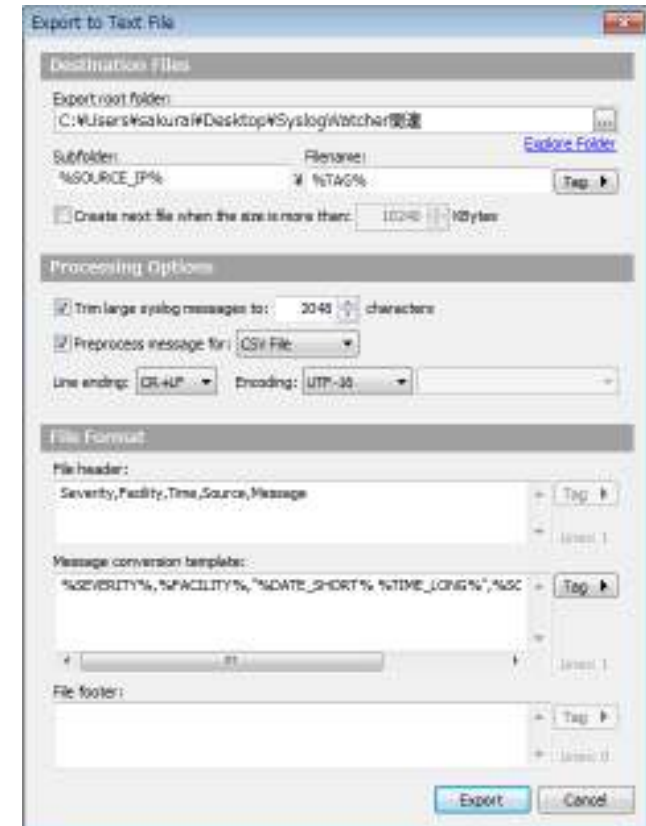
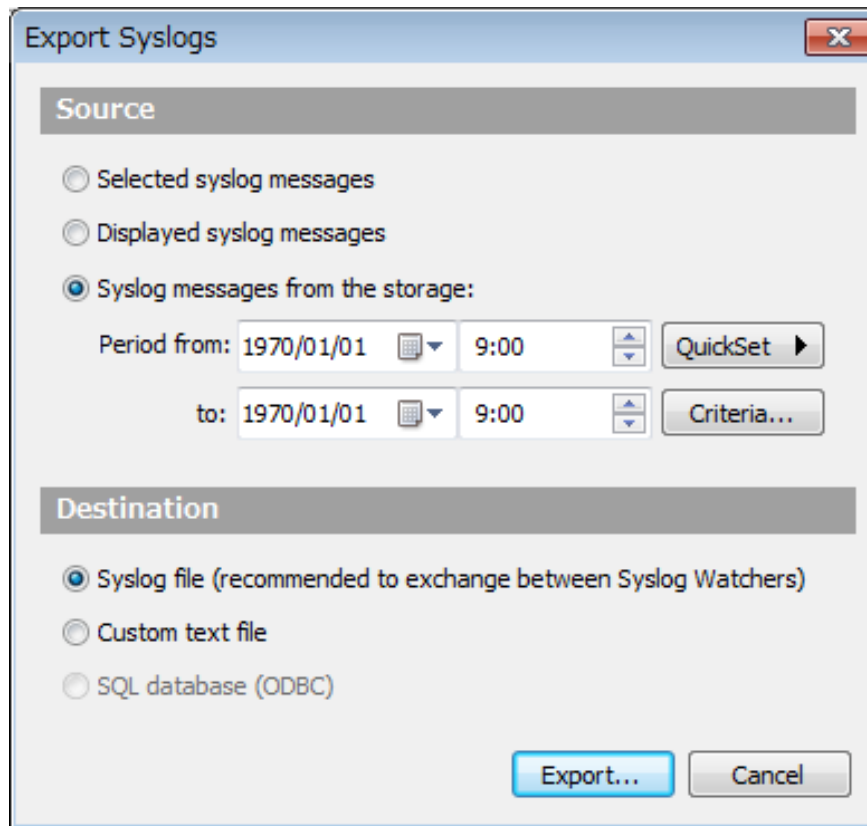
シスログストレージ③



シスログストレージはスケジュールバックアップが可能です。



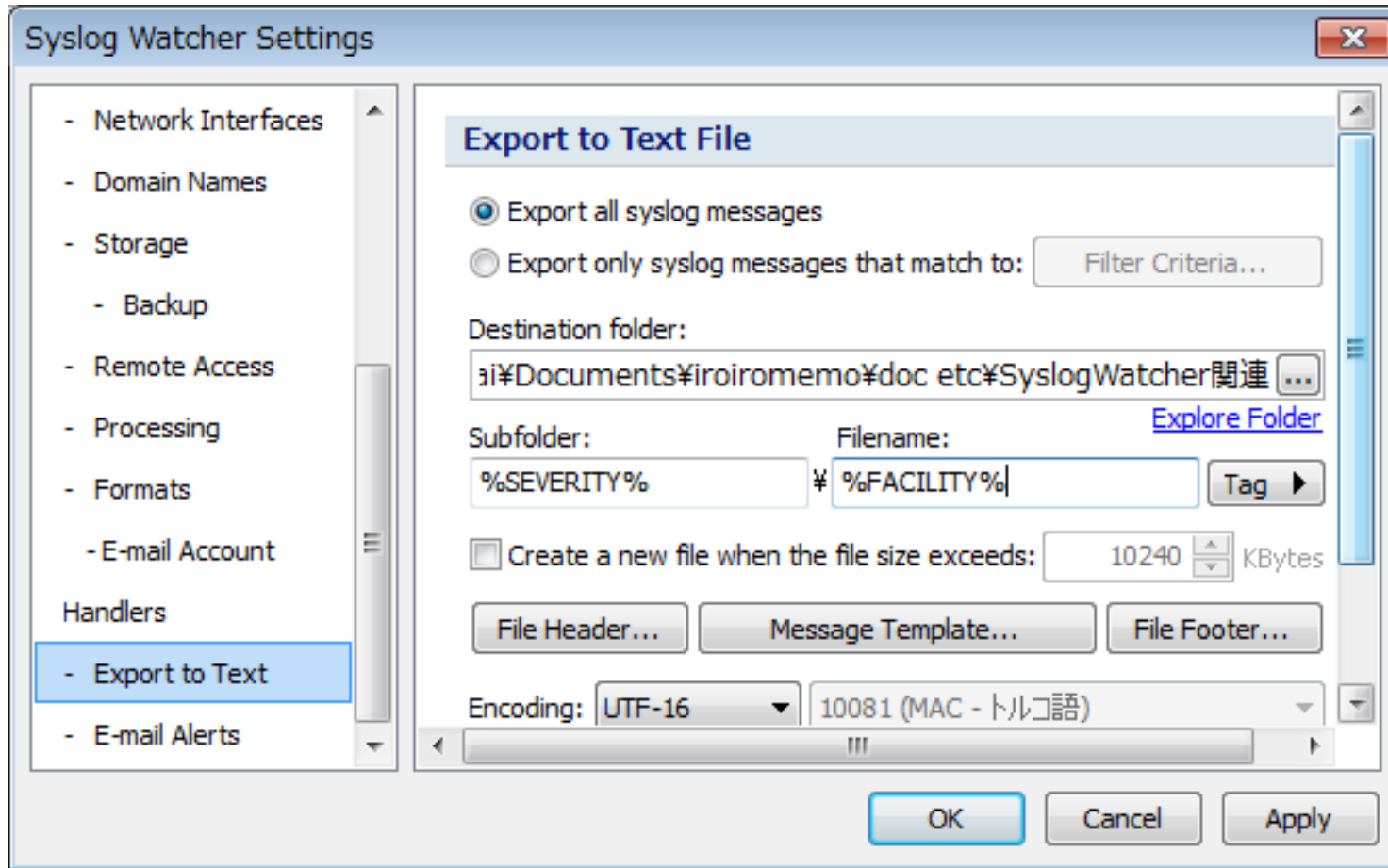
シスログエクスポート機能（手動）



SyslogWatcherで読み込み可能な”.syslog”ファイル形式、及び、カスタマイズされたtxtファイル形式で、シスログのエクスポートが可能です。



シスログエクスポート機能（自動）



Facility等を条件として、指定したフォルダにテキストファイルとしてシスログをリアルタイム保存することが可能です。



ベンダーパック アドオン

ベンダーパックアドオンは、SyslogWatcherでご利用いただける有料オプションです。Cisco Systems等対応機器が発行する独自のメッセージに対して、その説明と、適切な対応方法を表示できます。

対応機器

1. Cisco Systems, Inc.
 - Cisco IOS Software
 - Cisco Catalyst Switches
 - Cisco Security Appliances
2. Juniper Networks, Inc.
 - JUNOS Internet Software
3. Fortinet, Inc.
 - FortiGate with FortiOS

Message Details

10/06/07 09:43:07

Debug message from: 192.168.1.35

Hostname: MECOM

```
%PIX-7-710005: UDP request
discarded from 192.168.1.1/138 to
inside:192.168.1.255/netbios-dgm.
```

Interpretation

This message appears when the security appliance does not have a UDP server that services the UDP request. The message can also indicate a TCP packet that does not belong to any session on the security appliance. In addition, this message appears (with the service snmp) when the security appliance receives an SNMP request with an empty payload, even if it is from an authorized host. When the service is snmp, this message occurs a



その他

- ログの日時フォーマットのカスタマイズ。
- ログのIPアドレスをドメイン名に変更。
- 改行コードの除去などシスログの整形機能

他

● Override server settings ○ Use server settings

Date Format

● Use system date formats
○ Use custom format settings [Reset to Defaults](#)

Short date: First week day:

Long date:

Time Format

● Use system time formats
 Add milliseconds to long time format

Domain Names

Resolve IP address of syslog source to network name
 Look for IP addresses within message body and resolve them
 Use Fully Qualified Domain Name (FQDN)
 Use Relative Distinguished Name (RDN)

Cache resolved domain names for: hours