Sonarman User's Guide

Version 1.0

DevelUp Japan Corporation

<<Contents>>

はじめに

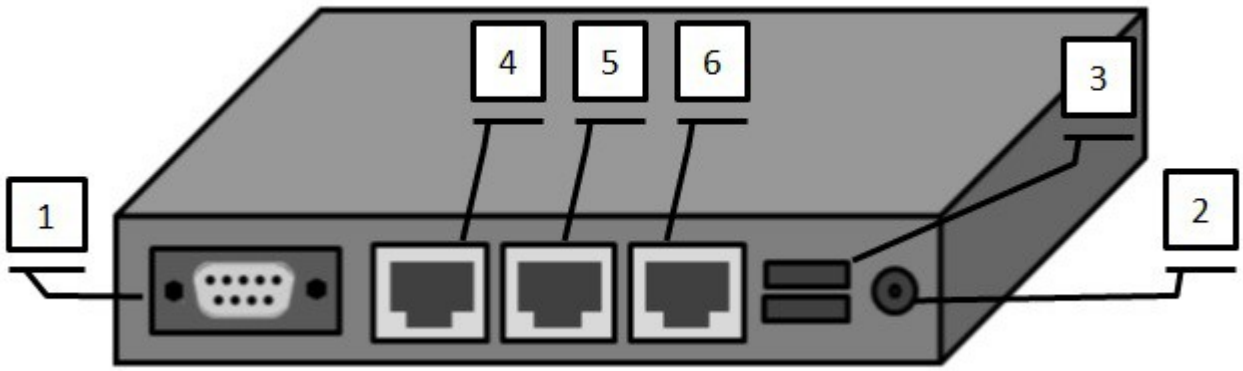
Sonarman（ソナーマン）は継続的にパケットキャプチャを取得するための製品です。
ソナーマンは以下のようなケースに最適です。

- 再現性の低いネットワーク障害の解決
- トラブルシューティングの効率を上げる
- ログ機能を補完する
- 証跡の保全を可能にする

説明

ソナーマンはネットワークの証跡としてのパケットをシンプルに扱うために開発されました。
ソナーマンはsyslogと連動し、パケットを保全するため、
問題が起きた時点の証跡を確実に保存することができます。
この製品が多くのシステム管理者の問題を減らす手助けとなることを望みます。

各部の名称



1 シリアルポート

ボーレートは 115200 です。

2 電源

DC 12V 0.5-1A 2.5mm

3 USB

4 Gigabit Ethenet eth0

WebUI, ssh, VPN supportなどの管理用ポートです。

5 Gigabit Ethenet eth1

パケットキャプチャ用ポートです。

6 Gigabit Ethenet eth2

パケットキャプチャ用ポートです。

Ethernetポートの左LEDは通信の発生に伴い点滅します。

右LEDはリンクのモードを示します。

Deploy

SetupGuide.mdを参照してください。

起動

ソナーマン付属の電源プラグを差し込んでください。

デフォルトではeth0はDHCPによりIPを取得します。

シリアルコンソールからIPアドレスを確認してください。

コンソールユーザーのアカウントは　sonarman/sonarman　です。

WebGUI

Access to http://ipaddress/

WEB画面のアカウントは admin/pass です。

Network configuration

Eth0 interface (IPv4)の設定を変更できます。

Change password

以下の画面でパスワードを変更できます。

Configure capture settings

サイズの数値は KB として扱われます。

ファイルサイズは 1M から 2G間での範囲で設定できます。

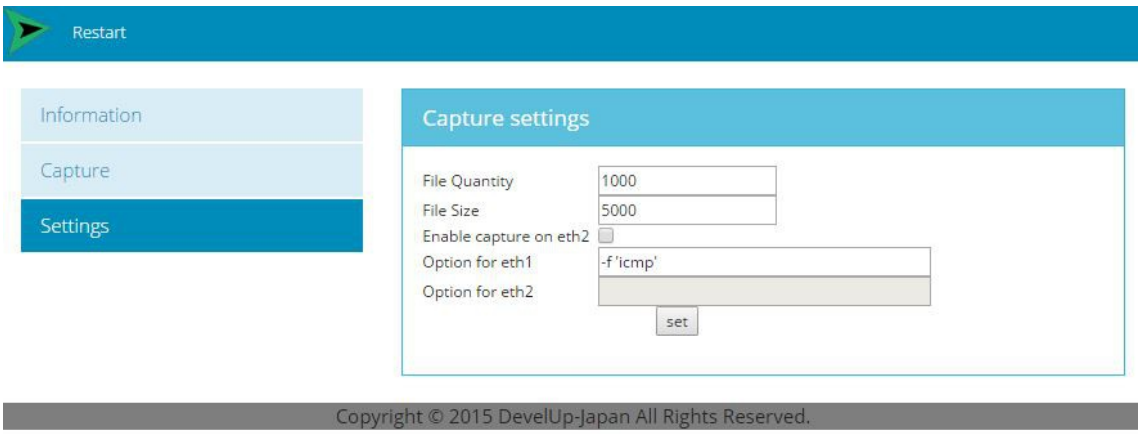
ファイルの個数は 10 から 100000までの範囲で設定できます。

これらの数値の最終合計はDISKサイズの80%までに制限されます。

Capture option　テキストボックスには　Tsharkのオプションを入力することができます。

Ex) -f 'ip.addr==192.168.1.1 && http'

例として上記のようなオプションを追加することができます。

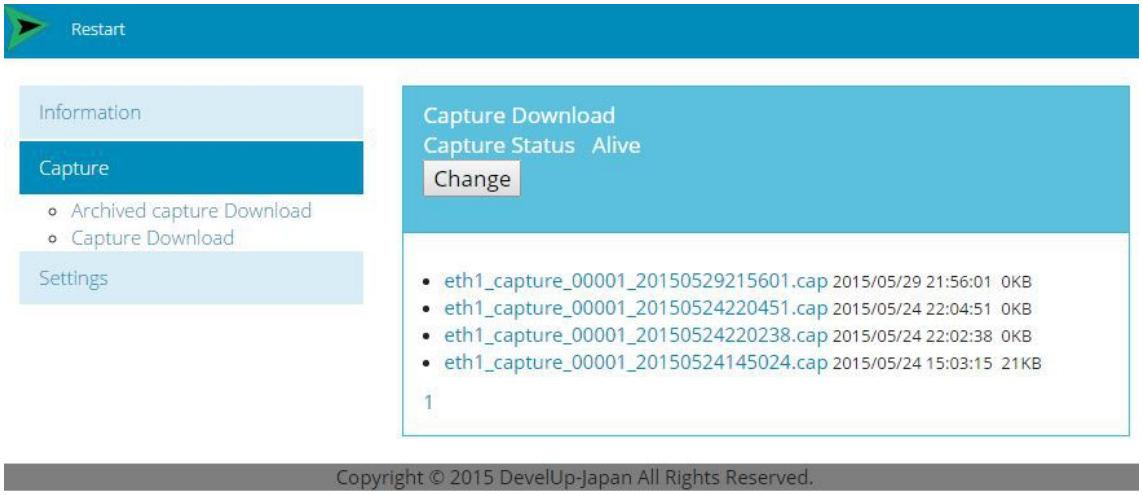


VPN Support

VPN機能はオープンソース版ではサポートされていません。

Capture file download

リングバッファに蓄積されているキャプチャファイルをダウンロードできます。
キャプチャファイルは一定時間経過後上書きされます。
キャプチャファイルを切り替えたい場合は"Change"ボタンを押してください。



Archived capture file download

Syslogメッセージによって退避されたアーカイブをダウンロードできます。
インターフェースごとに直前と一つ前のキャプチャファイルが保存されます。
保存のトリガーとなるsyslogメッセージは"ERRORINFO"です。

トリガーとなるsyslogキーワードを変更したい場合は /home/sonarman/shells/swatchrcを編集してください。

製品仕様

HW仕様	
型番	SM-001 (SMV-001 is virtual appliance edition)
大きさ(高さ X 幅 X 奥行 cm)	3.0X 16.8 X 15.7
接続ポート	Ethernet ×3, serial port (console) ×1, USB×2
Ethernet規格	IEEE 802.3u (10/100Mbps) IEEE 802.3ab (1000Mbps)
Memory	2G
AC電源	12V DC, 1A, 2.5 mm
ストレージ	SSD 128Gbyte(増設可)
CPU	AMD G-T40E (1GHz 2core x64 support)

FAQ

ソナーマンをどのようにしてネットワークに組み入れたらよいですか?

ソナーマンはL2スイッチのミラーリングポートでの使用を前提にしています。

リングバッファになるべく多くの記録を保持したい場合はフィルタオプションを併用してください。