

Sonarman User's Guide

Version 1.0

DevelUp Japan Corporation

<<Contents>>

○ 概要	P. 2
○ 製品説明	P. 3
○ 使用方法	P. 4
○ 製品仕様	P. 7
○ FAQ	P. 8

はじめに

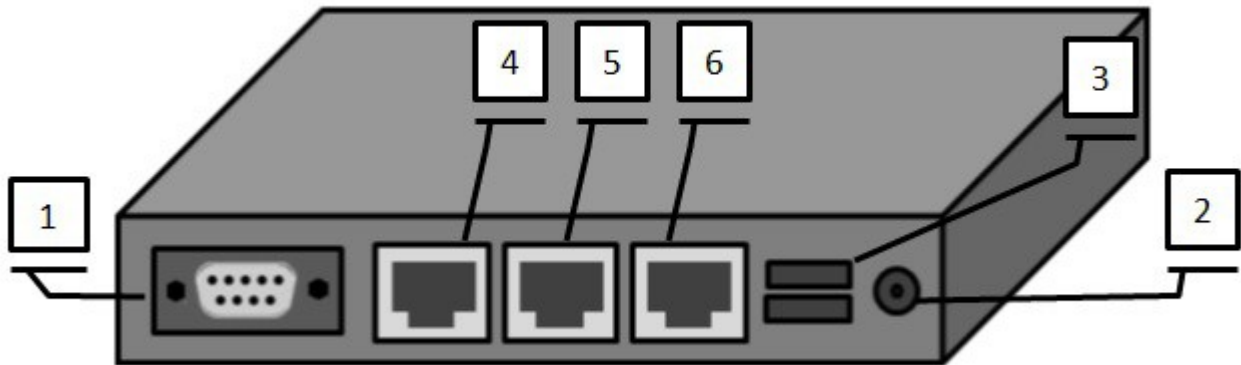
Sonarman（ソナーマン）は継続的にパケットキャプチャを取得するための製品です。
ソナーマンは以下のようなケースに最適です。

- 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 Ethernet eth0

WebUI, ssh, VPN supportなどの管理用ポートです。

5 Gigabit Ethernet eth1

パケットキャプチャ用ポートです。

6 Gigabit Ethernet 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。



Restart

Information

Capture

Settings

- IP settings
- Capture settings
- Password

IP settings

IP address

Netmask

Gateway

DHCP ☒ set

Copyright © 2015 DevelUp-Japan All Rights Reserved.

Change password

以下の画面でパスワードを変更できます。

The screenshot shows a web interface with a blue header bar containing a green play icon and the text "Restart". On the left, there is a sidebar with three menu items: "Information", "Capture", and "Settings" (which is highlighted in blue). Below "Settings" are three sub-items: "IP settings", "Capture settings", and "Password". The main content area is titled "Password" and contains a form with a "NewPassword" input field (masked with four dots), a checked checkbox labeled "Mask password", and a "set" button. At the bottom of the page, there is a grey footer bar with the text "Copyright © 2015 DevelUp-Japan All Rights Reserved."

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。

The screenshot shows a web interface with a blue header bar containing a green play icon and the text "Restart". On the left, there is a sidebar with three menu items: "Information", "Capture", and "Settings" (which is highlighted in blue). Below "Settings" are three sub-items: "IP settings", "Capture settings", and "Password". The main content area is titled "Capture settings" and contains a form with several input fields: "File Quantity" (1000), "File Size" (5000), "Enable capture on eth2" (checkbox), "Option for eth1" (-f 'icmp'), and "Option for eth2" (empty). A "set" button is located at the bottom right of the form. At the bottom of the page, there is a grey footer bar with the text "Copyright © 2015 DevelUp-Japan All Rights Reserved."

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。

Restart

Information

Capture

- Archived capture Download
- Capture Download

Settings

Capture Download

Capture Status: Alive

Change

- eth1_capture_00001_20150529215601.cap 2015/05/29 21:56:01 0KB
- eth1_capture_00001_20150524220451.cap 2015/05/24 22:04:51 0KB
- eth1_capture_00001_20150524220238.cap 2015/05/24 22:02:38 0KB
- eth1_capture_00001_20150524145024.cap 2015/05/24 15:03:15 21KB

1

Copyright © 2015 DevelUp-Japan All Rights Reserved.

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。

Restart

Information

Capture

- Archived capture Download
- Capture Download

Settings

Archived capture Download

- 20150529221607ERRORINFO.tar.gz 2015/05/29 22:16:07 8KB

1

Copyright © 2015 DevelUp-Japan All Rights Reserved.

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。

