2024/09/09

My work Log

T O C

[1.Proxmox 2](#_Toc178038509)

[A.ゲストOSに仮想化を公開する必要がある場合 2](#_Toc178038510)

[2.ubuntu 2](#_Toc178038511)

[A.Ubuntu インストールディスク作成 on Mac 2](#_Toc178038512)

[B.Ubuntu 2404 server install 2](#_Toc178038513)

[C.Cockpit install 3](#_Toc178038514)

[D.Docker install 3](#_Toc178038515)

[3.Fortigate 3](#_Toc178038516)

[A.ルーティング設定 3](#_Toc178038517)

[B.Syslog転送設定 4](#_Toc178038518)

[C.SNMP設定 4](#_Toc178038519)

[4.Cisco 5](#_Toc178038520)

[A.L2Switch - IP Address 5](#_Toc178038521)

[B.L2Switch - Syslog転送設定 5](#_Toc178038522)

[C.L2Switch - SNMP設定 6](#_Toc178038523)

[D.Mobility Express - Syslog転送設定 6](#_Toc178038524)

[E.Mobility Express - SNMP設定 6](#_Toc178038525)

[5.Juniper 6](#_Toc178038526)

[A.Syslog転送設定 6](#_Toc178038527)

[B.SNMP設定 6](#_Toc178038528)

[6.Datadog 6](#_Toc178038529)

[A.Agent 操作コマンド 6](#_Toc178038530)

[B.SNMPモニタリング 7](#_Toc178038531)

[C.Ping Check 7](#_Toc178038532)

[D.デバイストポロジー 9](#_Toc178038533)

[7.Zabbix 9](#_Toc178038534)

[8.New relic 9](#_Toc178038535)

[9.ログ監視 9](#_Toc178038536)

[A.rsyslog 9](#_Toc178038537)

[i. Install 9](#_Toc178038538)

[ii. IPアドレスごとにログファイルを振り分ける設定 10](#_Toc178038539)

[B.Graylog 11](#_Toc178038540)

[i. Install 11](#_Toc178038541)

[ii. Syslog取り込み設定 11](#_Toc178038542)

[C.rsyslog -> Graylogへのログ転送 11](#_Toc178038543)

[i. rsyslogの設定 11](#_Toc178038544)

[10.Tips! 11](#_Toc178038545)

[A.Docker 11](#_Toc178038546)

[i. Docker-composeとかやりすぎて、ゴミを一掃したいとき 11](#_Toc178038547)

[ii. 読み書き権限問題。サービスをRoot権限で起動したいとき 12](#_Toc178038548)

# Proxmox

## ゲストOSに仮想化を公開する必要がある場合

1. 仮想マシン作成時に以下の設定を実施

BIOS：OVMF(UEFI)

プロセッサ：host

# ubuntu

## Ubuntu インストールディスク作成 on Mac

CUIで行う

[MacでUbuntu Server ImageをダウンロードしてUSBに設定する方法](https://zenn.dev/pon24/articles/bf17cf7a6cd910)

参考

* [MacでUbuntu Server ImageをダウンロードしてUSBに設定する方法](https://zenn.dev/pon24/articles/bf17cf7a6cd910)

## Ubuntu 2404 server install

1. 論理ボリュームの選択 <- LVMを無効化
2. UFWをインストール
3. Remote Desktop設定

参考

* [Ubuntu で Gufw を用いてファイアウオール](https://www.kkaneko.jp/tools/server/gufw_ubuntu.html)

## Cockpit install

1. KVMのインストール
2. Cockpitのインストール
3. Firewall設定（0.0.0.0 を変更して、アクセス元IPを制限する）

sudo ufw allow from 0.0.0.0/0 to any port 9090 proto tcp

1. Cockpitへのアクセス
2. 仮想ブリッジの作成

参考

* [Ubuntu 24.4で自宅サーバ（KVMとCockpitで仮想サーバ編）[2/6]](https://www.smarthome-diy.info/blog/developper/smarthome/2024/05/3807/%20%20https:/www.kkaneko.jp/tools/server/gufw_ubuntu.html%20%20https:/higmasan.com/almalinux/kvm%E4%BB%AE%E6%83%B3%E3%83%9E%E3%82%B7%E3%83%B3%E3%82%92%E3%83%96%E3%83%AA%E3%83%83%E3%82%B8%E6%8E%A5%E7%B6%9A%E3%81%99%E3%82%8B/)

## Docker install

手順通りにコマンドを打つだけ

参考

* [Ubuntu 22.04でDocker、DockerComposeをインストールする](https://arkgame.com/2022/04/29/post-307627/)

# Fortigate

## ルーティング設定

FortiGateでは、デフォルトで直接接続間はルーティングされるので、I Pv4ポリシでセグメント間通信を許可すればO K

1. IPv4ポリシ作成



グラフィカル ユーザー インターフェイス, アプリケーション

自動的に生成された説明

## Syslog転送設定

GUIで設定

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, メール

自動的に生成された説明

参考

* [FortiGateにおける複数のSyslogサーバへログ転送を行う設定について](https://www.secuavail.com/kb/tech-blog/tb-210428_01/%20%20https:/cloud.freebit.com/support/faq/vdc/37158/)

## SNMP設定

GUIで設定

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, メール

自動的に生成された説明

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション

自動的に生成された説明

# Cisco

## L2Switch - IP Address

1. Vlan interfaceに対して、ip Addressを割り振るだけ

#conf t

#interface vlan 11

#Ip address 192.168.11.251 255.255.255.0

#no shutdown

## L2Switch - Syslog転送設定

参考

* [Cisco 製品にSNMP (v1, v2c) / Syslog の設定を追加する (Cisco Catalyst, ASA, Router )](https://www.secuavail.com/kb/tech-blog/tb-190205_02/)

## L2Switch - SNMP設定

1. SNMPポーリング設定を一行追加するだけ

#conf t

#snmp-server community SNMPCommunity ro

## Mobility Express - Syslog転送設定

## Mobility Express - SNMP設定

1. SNMPポーリング設定を一行追加するだけ

GUIで設定

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, チャットまたはテキスト メッセージ

自動的に生成された説明

# Juniper

## Syslog転送設定

## SNMP設定

# Datadog

## Agent 操作コマンド

| 説明 | コマンド |
| --- | --- |
| Agent をサービスとして起動 | sudo service datadog-agent start |
| サービスとして実行中の Agent の停止 | sudo service datadog-agent stop |
| サービスとして実行中の Agent の再起動 | sudo service datadog-agent restart |
| Agent サービスのステータス | sudo service datadog-agent status |
| 実行中の Agent のステータスページ | sudo datadog-agent status |
| フレアの送信 | sudo datadog-agent flare |
| コマンドの使用方法の表示 | sudo datadog-agent --help |
| チェックの実行 | sudo -u dd-agent -- datadog-agent check <CHECK\_NAME> |

参考

* [Ubuntu 用 Agent の基本的な使用方法](https://docs.datadoghq.com/ja/agent/basic_agent_usage/ubuntu/)

## SNMPモニタリング

1. sudo nano /etc/datadog-agent/conf.d/snmp.d/conf.yaml

init\_config:

loader: core # use core check implementation of SNMP integration. recommended

use\_device\_id\_as\_hostname: true # recommended

instances:

- ip\_address: '192.168.11.1'

community\_string: 'Private01' # enclose with single quote

tags:

- 'host\_name\_TDD1:FortiGate50E'

- 'ip\_address\_TDD1:192.168.11.1'

ping:

enabled: true # (default false) enable the ping check

linux: # (optional) Linux specific configuration

use\_raw\_socket: true # (optional, default false) send pings using a raw socket (see step 3 above)

- ip\_address: '192.168.11.251'

community\_string: 'Private01' # enclose with single quote

tags:

- 'host\_name\_TDD1:C2960L'

- 'ip\_address\_TDD1:192.168.11.251'

ping:

enabled: true # (default false) enable the ping check

linux: # (optional) Linux specific configuration

use\_raw\_socket: true # (optional, default false) send pings using a raw socket (see step 3 above)

参考

* [ネットワークデバイスから SNMP メトリクスを収集 - Ping](https://docs.datadoghq.com/ja/network_monitoring/devices/snmp_metrics/?tab=individual#ping)

## Ping Check

1. Agent Integrationのインストール
2. conf.yaml作成

sudo nano /etc/datadog-agent/conf.d/ping.d/conf.yaml

init\_config:

instances:

## @param host - string - required

## Host to ping

#

- host: 192.168.11.1

## @param collect\_response\_time - boolean - optional - default: false

## Reports network.ping.response\_time in ms if true

#

collect\_response\_time: true

## @param timeout - float - optional - default: 4.0

## Timeout in seconds

#

timeout: 5.0

## @param tags - list of key:value elements - optional

## List of tags to attach to every metric, event and service check emitted by this integration.

##

## Learn more about tagging: https://docs.datadoghq.com/tagging/

#

tags:

- 'host\_name\_TDD1:FortiGate50E'

- 'ip\_address\_TDD1:192.168.11.1'

1. Agent Restart

失敗の場合

テキスト が含まれている画像

自動的に生成された説明

成功の場合

テキスト

自動的に生成された説明

参考

* [Ping インテグレーション](https://docs.datadoghq.com/ja/integrations/ping/)

## デバイストポロジー

グラフィカル ユーザー インターフェイス が含まれている画像

自動的に生成された説明

参考

* [Device Topology Map](https://docs.datadoghq.com/ja/network_monitoring/devices/device_topology_map)

# Zabbix

# New relic

# ログ監視

<前提条件>

rsyslog server宛にsyslogを送付している（Fortigateなどから）

## rsyslog

### Install

[Syslogサーバ(UDP)のInput設定](https://qiita.com/h_tyokinuhata/items/c6733aed3a576a78a38b)

UDPポート514番でリッスンして外部からのログを受け付ける設定

外部からのアクセスの場合は /var/log/remote にログを保存する設定

ufwは有効化しない

テキスト

自動的に生成された説明

### IPアドレスごとにログファイルを振り分ける設定

送信ホストのIPアドレスごとに自動的にファイルを作成し、ログの書き込みファイルを振り分けるの設定

1. rsyslogの設定ファイルを編集: /etc/rsyslog.conf ファイルを編集します。

sudo nano /etc/rsyslog.conf

1. 以下の行を追加してください。

$RepeatedMsgReduction off

これにより、同じメッセージが繰り返し書き込まれないようになります。

1. ログの振り分け設定: /etc/rsyslog.d/ ディレクトリ内に、送信ホストごとにログを振り分ける設定ファイルを作成します。例えば、/etc/rsyslog.d/20-remote-hosts.conf という名前のファイルを作成します。
2. sudo nano /etc/rsyslog.d/20-remote-hosts.conf に以下を記述

template(name="HostBasedLog" type="string" string="/var/log/%FROMHOST-IP%.log")

\*.\* ?HostBasedLog

この設定では、%FROMHOST-IP% プロパティを使って送信ホストのIPアドレスを取得し、それをログファイル名に含めます。

1. rsyslog の再起動: 設定を反映させるために、rsyslog を再起動します。

sudo service rsyslog restart

これで、送信ホストのIPアドレスごとに自動的にファイルを作成し、ログの書き込みファイルを振り分ける設定が完了しました。

参考

* [Syslogサーバ(UDP)のInput設定](https://qiita.com/h_tyokinuhata/items/c6733aed3a576a78a38b)

## Graylog

### Install

Docker install

[ログ分析管理OSS(Graylog-6.0.3)のDocker実行Tips](https://qiita.com/khat/items/15da5859b09725adb819)

### Syslog取り込み設定

Syslogサーバ(UDP)のInput設定

[ログの受信設定をするには(Input設定)](https://www.designet.co.jp/ossinfo/graylog/manual/input.php#syslog-udp-input)

参考

* [ログ分析管理OSS(Graylog-6.0.3)のDocker実行Tips](https://qiita.com/khat/items/15da5859b09725adb819)
* [ログの受信設定をするには(Input設定)](https://www.designet.co.jp/ossinfo/graylog/manual/input.php#syslog-udp-input)
* [Graylog日本語マニュアル](https://www.designet.co.jp/ossinfo/graylog/manual/)
* [Getting Started - Graylog v1.x](https://gettingstarted.graylog.org/assets/v1/index.html?c=&v=&o=)
* [ログ監視ツールについて調べてみた](https://speakerdeck.com/nearme_tech/rogujian-shi-turunituitediao-betemita?slide=27)

## rsyslog -> Graylogへのログ転送

### rsyslogの設定

1. sudo vim /etc/rsyslog.d/50-forward.conf

$ModLoad imudp

$UDPServerRun 514

$ActionQueueType LinkedList # use asynchronous processing

$ActionQueueFileName srvrfwd # set file name, also enables disk mode

$ActionResumeRetryCount -1 # infinite retries on insert failure

$ActionQueueSaveOnShutdown on # save in-memory data if rsyslog shuts down

\*.\* @192.168.11.204:5140;RSYSLOG\_SyslogProtocol23Format

★＠一つ：UDP, @二つ：TCP

参考

* [rsyslogで取得したログを直接fluentdに送る](https://qiita.com/tjinjin/items/2bb36c7960a69bf42e2d)
* [fluentdのsyslogプラグインを使ってsyslogプロトコルでログを受け取る](https://d.docs.live.net/f3157fbed5eccb88/%09https:/qiita.com/suzuki-navi/items/2410ebdf92279996c516)
* [rsyslogサーバで外部からのログを受け付ける](https://qiita.com/h_tyokinuhata/items/c6733aed3a576a78a38b)

# Tips!

## Docker

### Docker-composeとかやりすぎて、ゴミを一掃したいとき

<https://docs.docker.jp/config/pruning.html>

既存のコンテナ～使われていないイメージすべてを削除するには、 -a フラグを使います。

$ docker image prune -a

WARNING! This will remove all images without at least one container associated to them.

Are you sure you want to continue? [y/N] y

### 読み書き権限問題。サービスをRoot権限で起動したいとき

<https://www.oresamalabo.net/entry/2019/03/09/120747>

解決策

→ td-agentサービス を root ユーザーで起動する。

td-agent のログを確認すると、`Permission denied` というメッセージが毎秒出力されている事がわかり、実行ユーザーの権限に問題があるのではないかという仮説が立てられます。