

評価ガイド

ntopng and nProbe

Rev2.0

2024年1月4日



ジュピターテクノロジー

版	発行日	変更内容
第 1.0 版	2020/02/07	初版作成
第 1.1 版	2020/02/13	ntopng and nProbeのモデルを追加
第 1.3 版	2020/04/28	OVAを提供する方式に変更。評価は、Oracle VB + ovaに統一した
第 1.4 版	2020/6/15	™の削除, p6にisoファイルリリースのリンクを追加
第 1.5 版	2022/10/03	GPGキー変更に伴うアップグレード方法を追記
第 2.0 版	2024/1/4	v6.0リリース及び新規ISOリリースに伴う変更

- ntopng及びnProbeはntop社の商標です。
- その他記載されている会社名、製品名、商品名は各社の商標または登録商標です。

ntop社 ntopng及びnProbeの評価をご検討頂き、 誠にありがとうございます。

本ガイドではntop社の両製品を評価していただく為に、インストール・基本的な設定手順及び留意事項を説明いたします。

目次

1. はじめに
2. 評価版について
3. ISOファイルによるインストール
4. ntopngのインストール
5. NIC直接監視評価パターン
6. ntopng Enterprise版評価方法
7. ntopng NIC直接監視評価 基本画面説明
8. ntopng+nProbe xFlow受信評価パターン
9. お問い合わせ先

ntop社のntopng及びnProbeは、高速でトラフィック情報を分析し対象ネットワークの監視を実現する製品です。製品ごとに役割が異なります。以下に製品概要を説明します。

- ntopng・・・リアルタイム性が高いL7高速トラフィック分析を実現し、フローコレクターとして長期のトラフィック分析ができます。ルーターやスイッチのミラーポート、もしくはRITEポート、TAPと直接接続することで、高速のトラフィック分析ツールとして動作します。また、nProbeと連携することで監視対象ルーターが分散した環境でもNetFlow v5,v9/IPFIXによるトラフィック分析が可能となる高速トラフィック分析ツールです。
- nProbe・・・xFlowに対応していないルーターを補助するNetFlowプローブ製品です。モードが3種類あり、NetFlowプローブのProbeモード、MySQL/DiskにNetFlowデータを収集するコレクタモード、受信したxFlowをNetFlow v5,v9/IPFIXに変換してコレクタに送信するProxyモードの3モードをサポートします。

本評価ガイドでは、Vmware Workstation Player/物理環境で各製品の評価ができるよう、ご紹介しております。

2. ntopng and nProbe 評価版について

- ◆本評価マニュアルでは、弊社が提供するISOファイルを使って、VMware Workstation/物理環境上に評価環境をセットアップする方法をご紹介します。

注意)インストールは、インターネット環境が必須となります。

- ◆評価版利用上の注意

ntopngは起動から10分間経過するとコミュニティ版にダウングレード、nProbeは25,000フローを受信した時点でフローの受信を停止します。有償版での検証を進めるには、適宜それぞれのプロセスを定期的に再起動して、ご評価願います。

- ◆評価用ISOファイルの入手について

評価版ISOファイルのご利用は、弊社までお申し込み下さい。

[評価版リクエストサイト]

<https://www.jtc-i.co.jp/support/download/>

- ◆ ntopng及びnProbeのISOをインストールするシステム要件は、以下の通りです。

CPU	メモリ	HDD
2コア以上の割り当て	4GB以上の割り当て	20GB以上の割り当て

上記記載の要件はISO評価版を動作させるのに必要な最低要件となります。高負荷環境を想定しているシステム要件ではございませんので、ご注意ください。

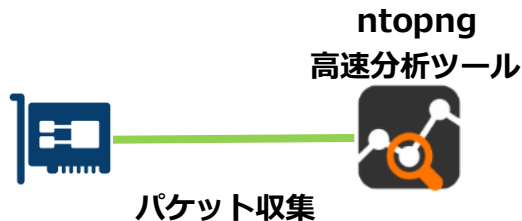
ntopngにアクセスする場合は、WEBブラウザが必要となります。
弊社では、Google Chromeの最新版を推奨いたします。

弊社が提供するISOファイルを使ってインストールすれば、以下の2パターンの評価が出来ます。1つ目は自PCのNICを流れるトラフィックを監視をする「NIC直接監視」の評価。2つ目は、NetFlowやsflowを受信する「xFlow受信」の評価となります。

評価パターン①

ntopngのNIC直接監視の評価

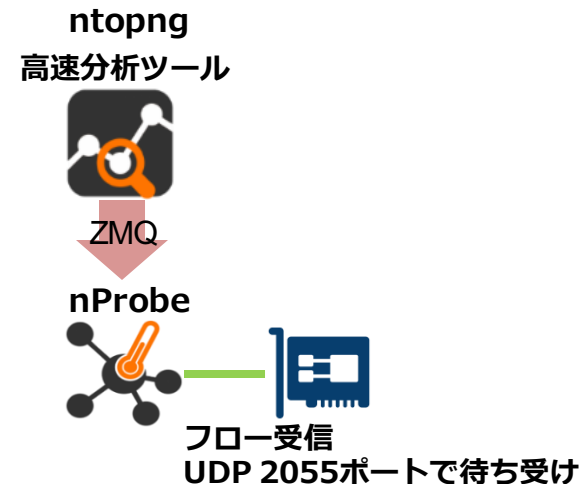
※本評価ドキュメントの5章～7章までの
評価環境



評価パターン②

ntopng+nProbe xFlow受信の評価

※本評価ドキュメント8章の評価環境

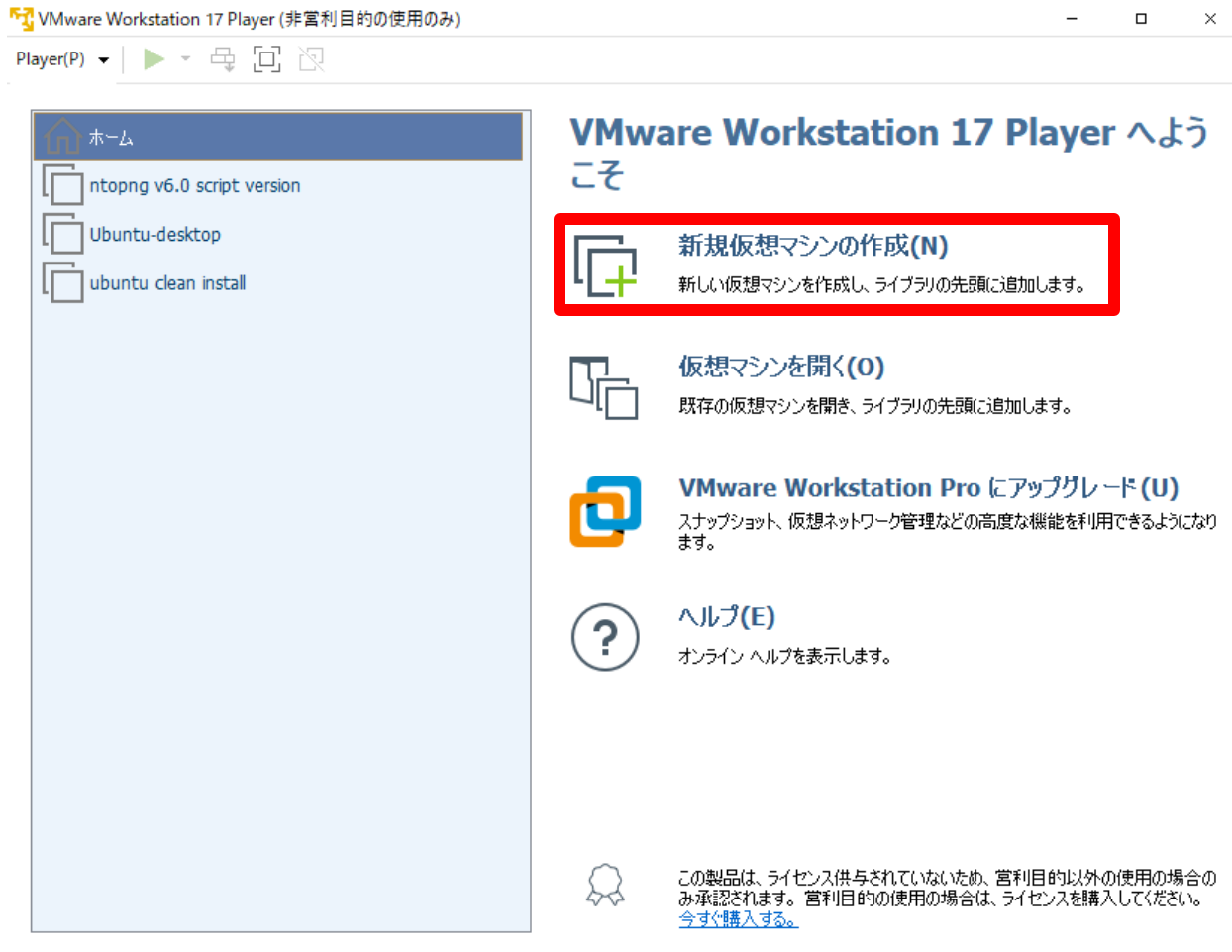


3. ISOインストール

本章では以下のバージョンを使用しています。

- ◆ Windows 11 x64
 - ◆ nProbe 10.X and ntopng v6.X Stable版
 - ◆ VMware Workstation 17
-

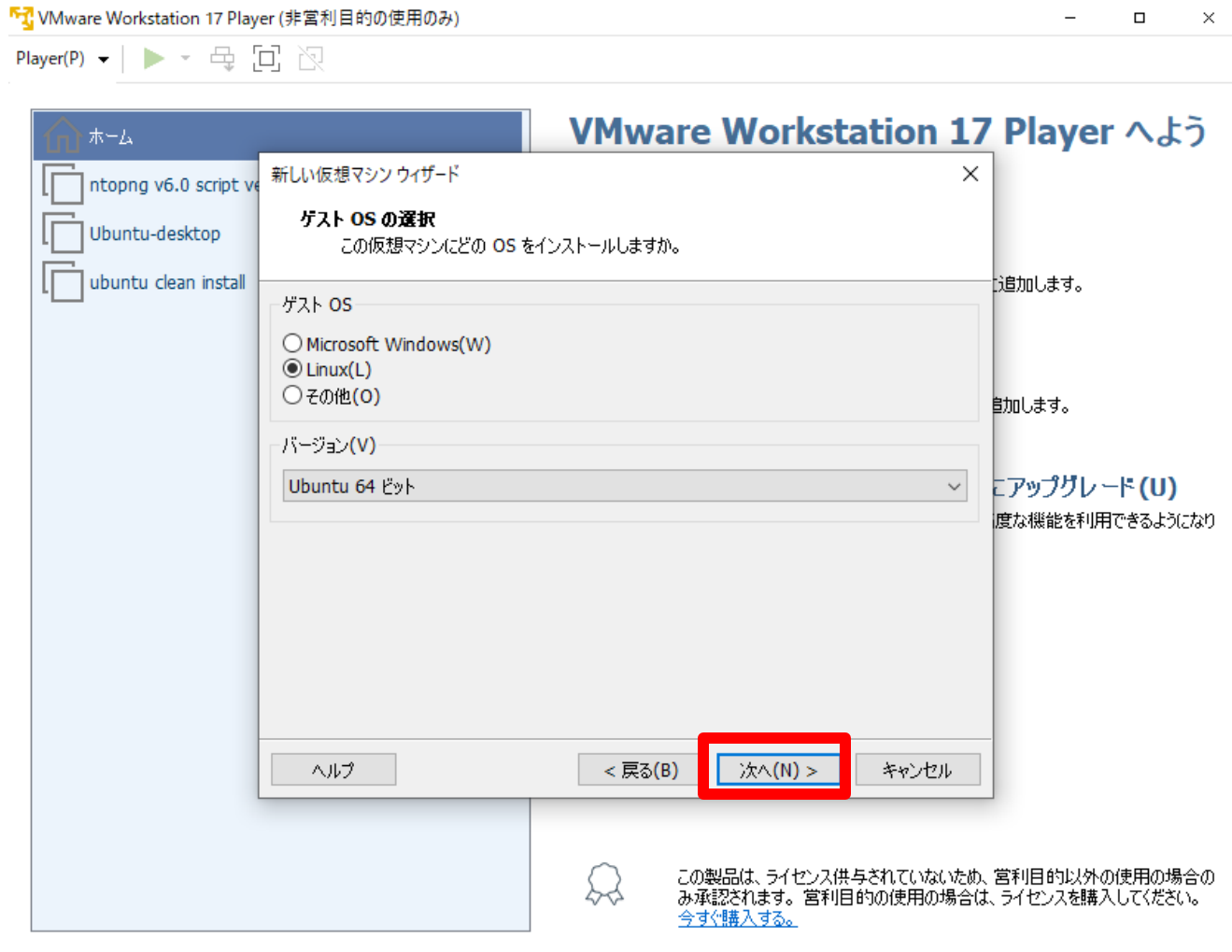
「新規マシンの作成(N)」をクリックしてください。



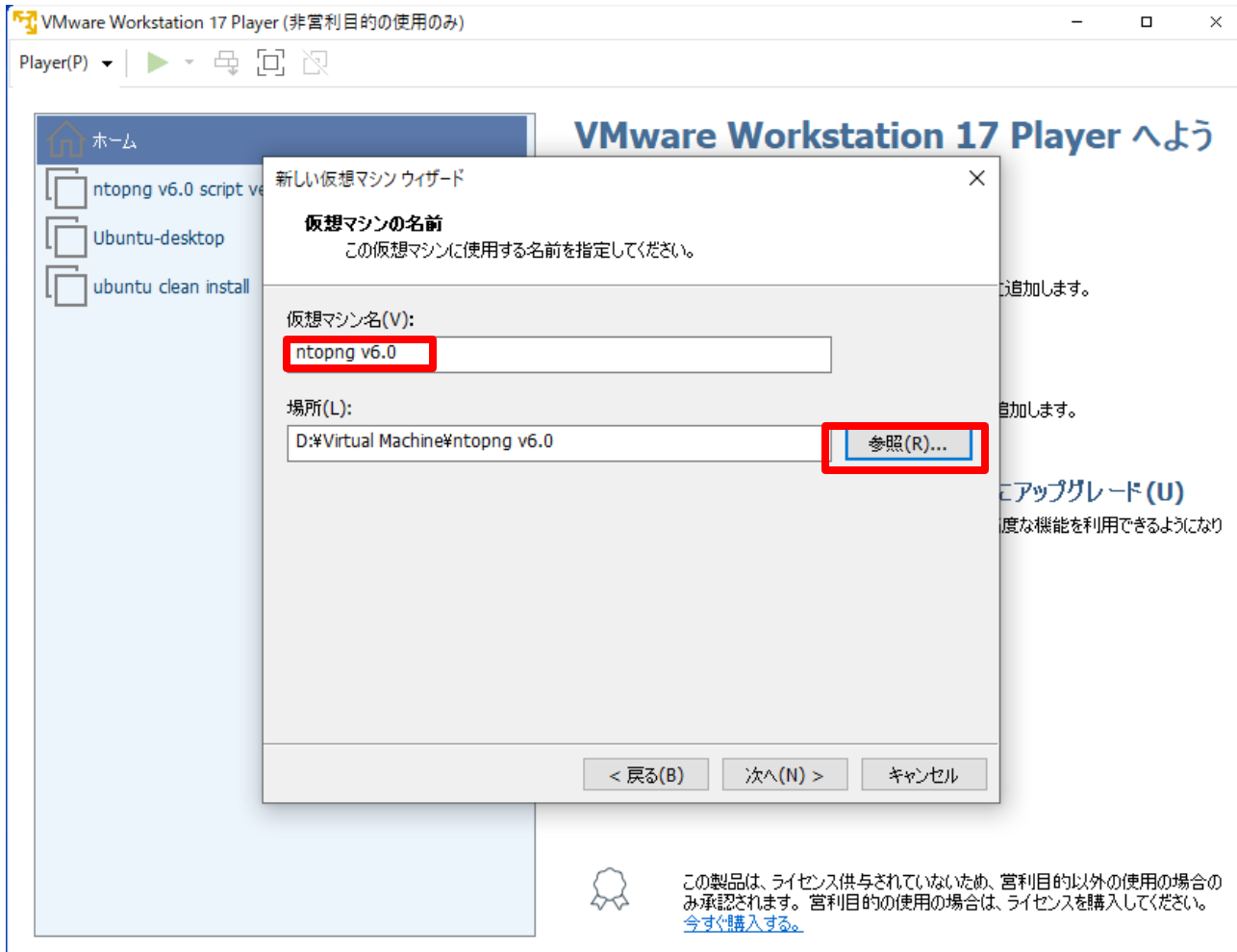
「参照(R)」をクリックし、弊社サイトからダウンロードしたisoファイルを選択して、「次(N)>」をクリックします。



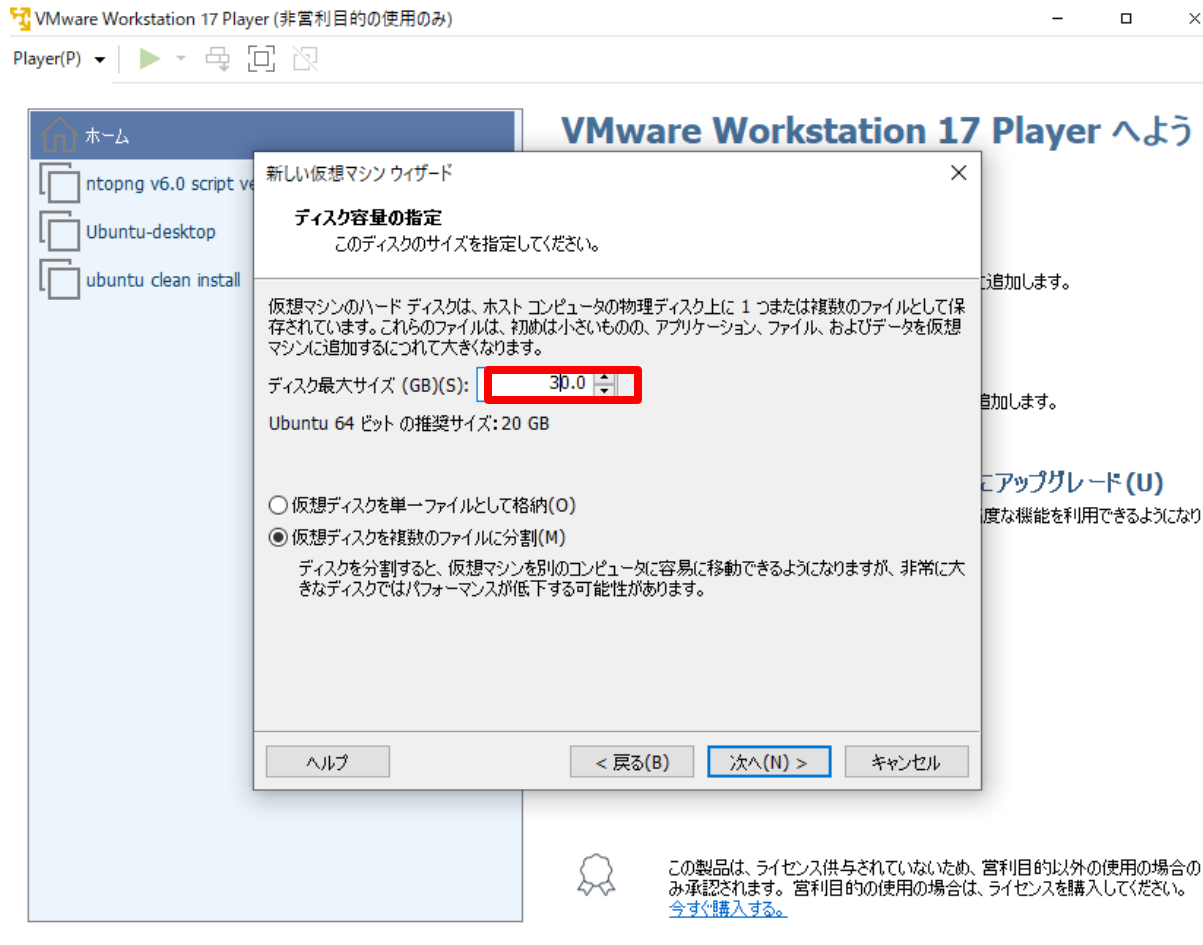
「Linux(L)」、「Ubuntu 64ビット」が選択されていることを確認し、「次(N)>」をクリックします。



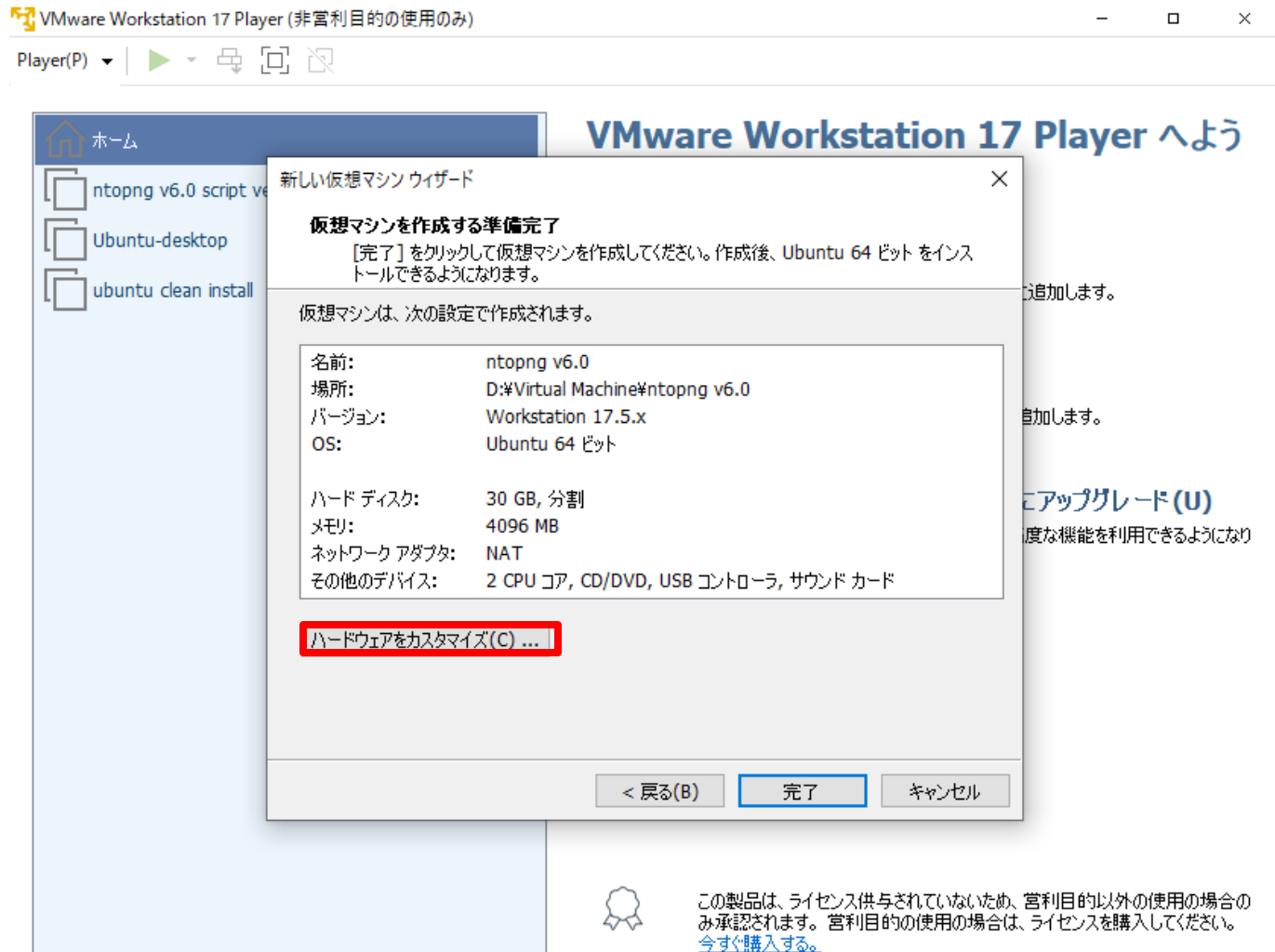
仮想マシン名に任意の名称、場所には仮想マシンを保存するディレクトリを指定してください。
「次(N)>」をクリックします。



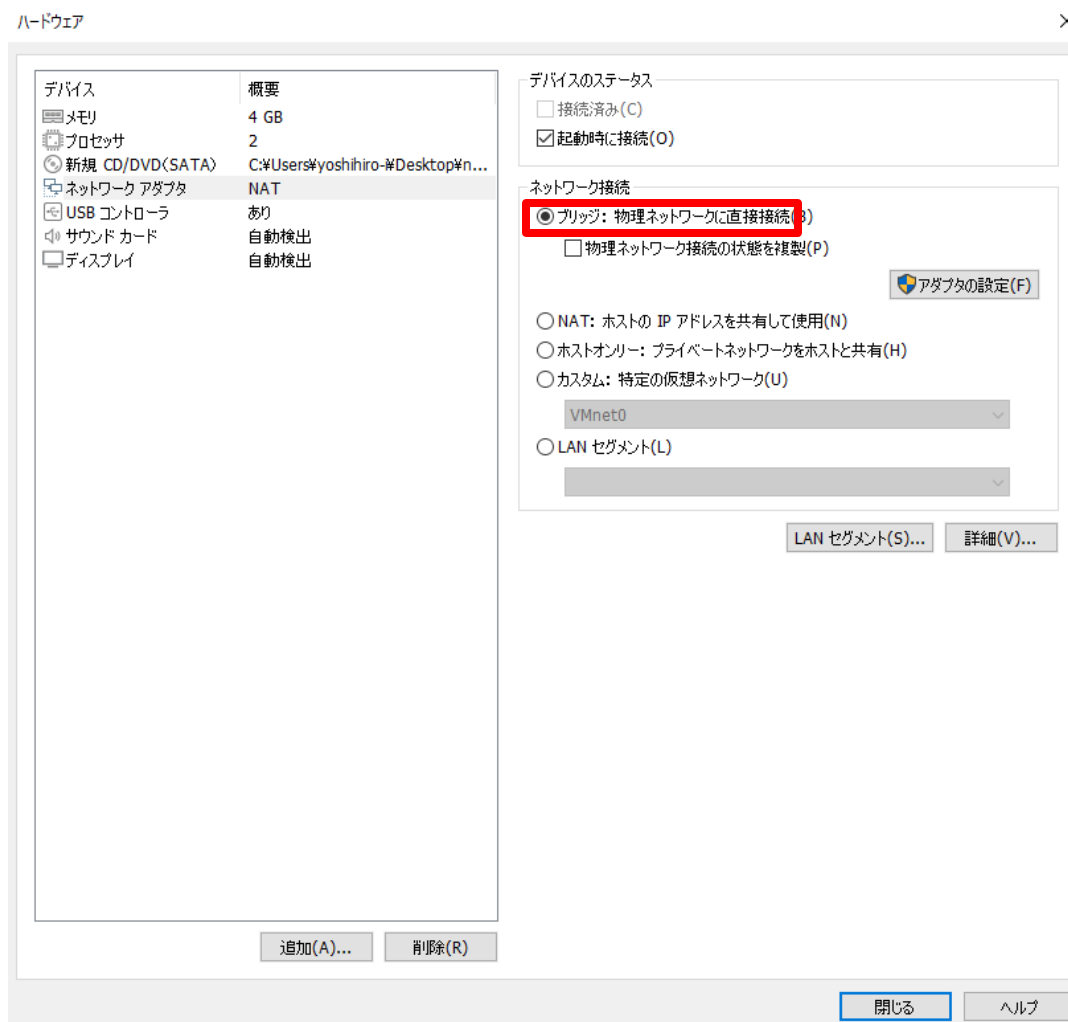
ディスク最大サイズ(GB)(S)を30.0に設定し、「次(N)>」をクリックします。



ハードウェアをカスタマイズ(C)... をクリックします。



ブリッジをクリックし、「閉じる」ボタンをクリックします。



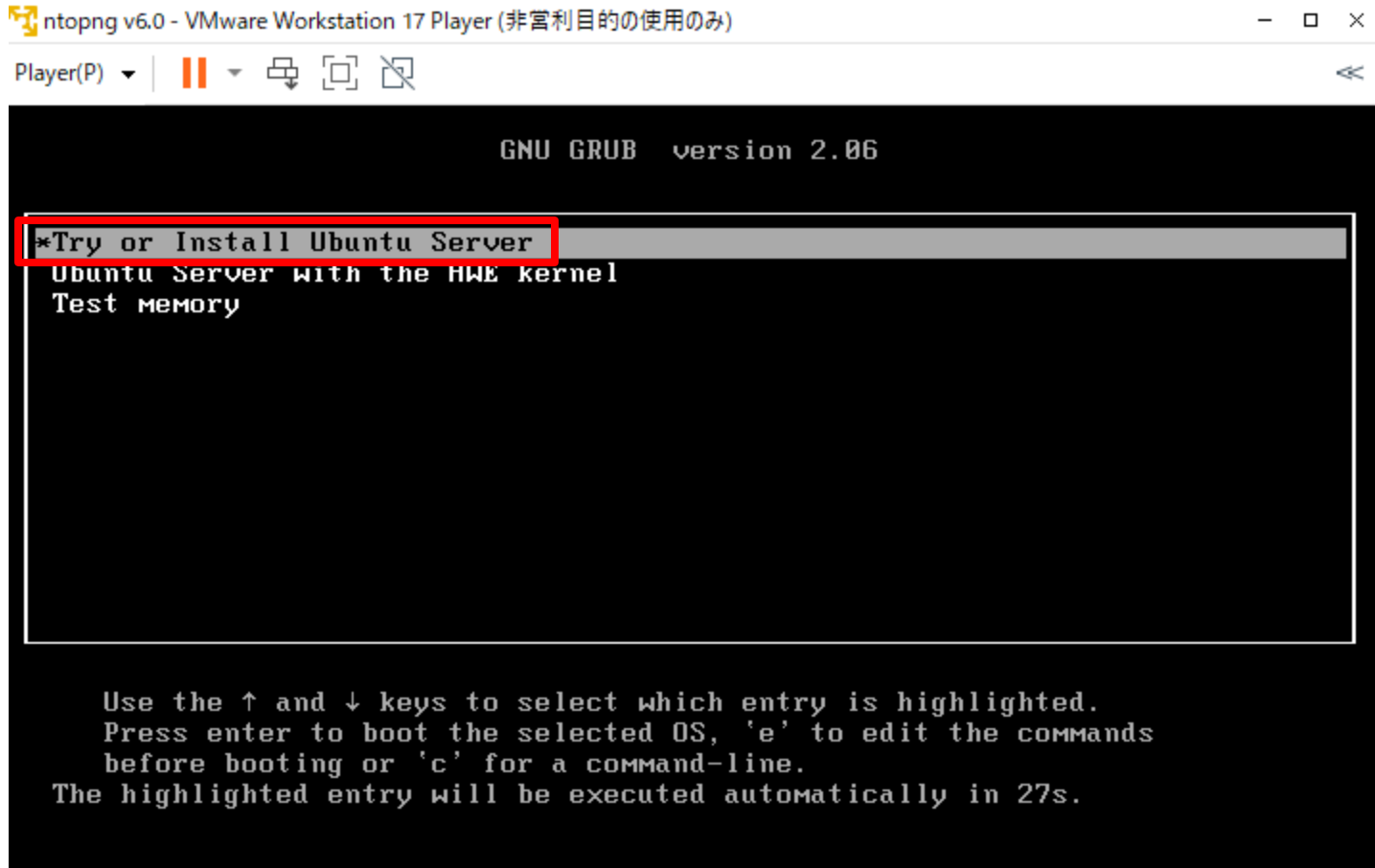
ネットワークアダプタが、「ブリッジ(自動)」になっていることを確認し、「完了」ボタンをクリックします。



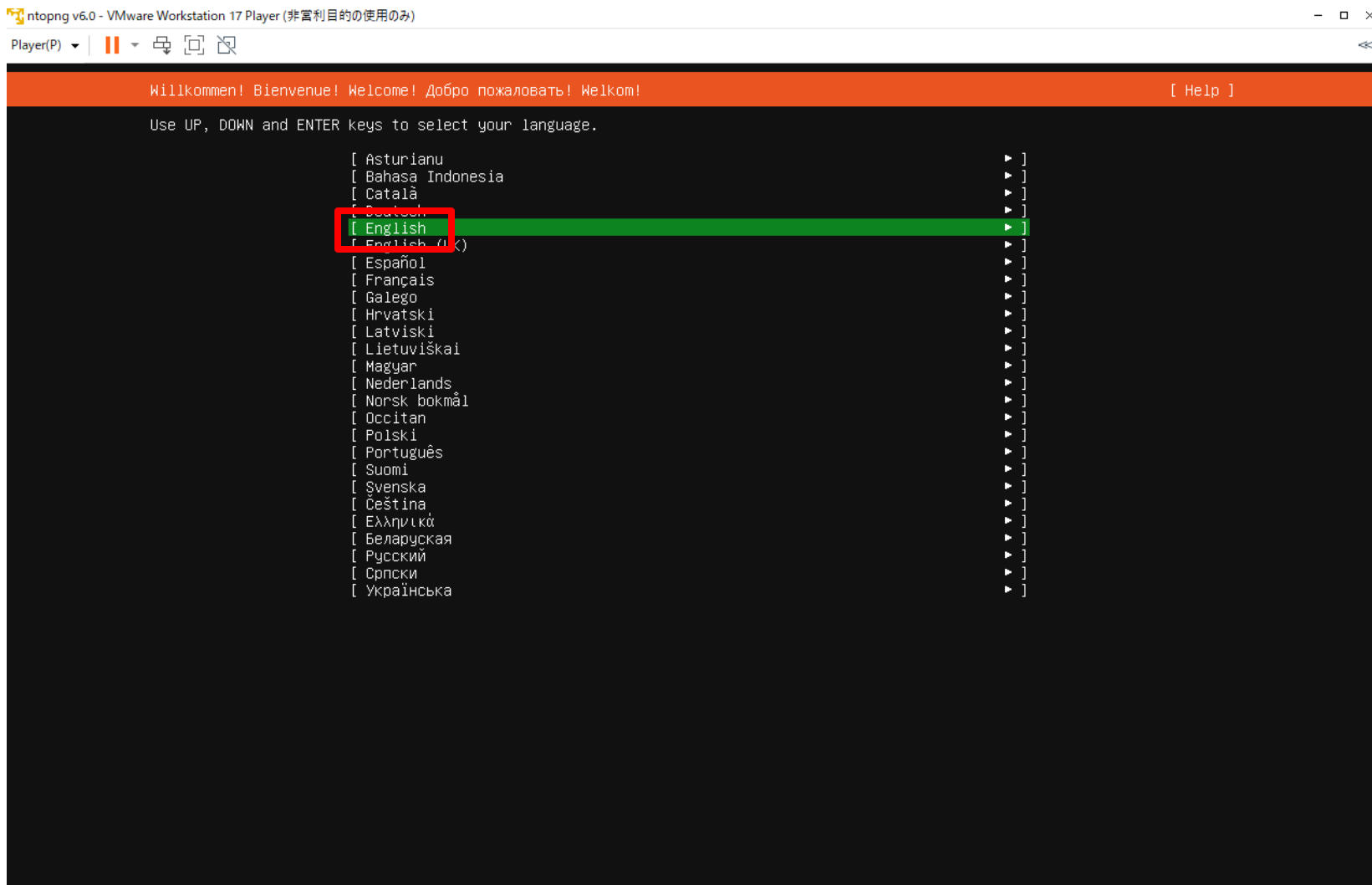
「仮想マシンの再生(L)」ボタンをクリックします。



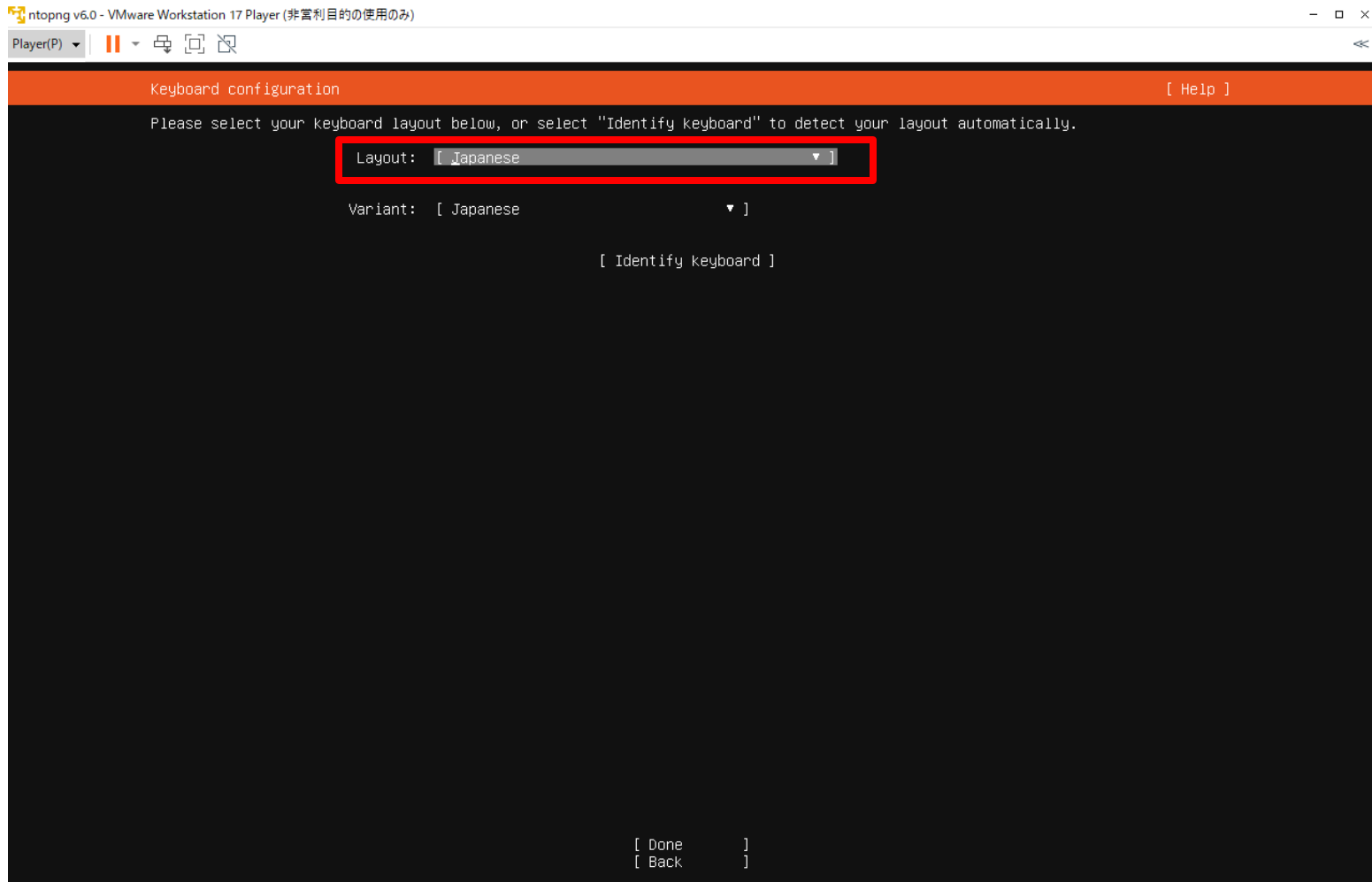
「*Try or Install Ubuntu Server」が選択されていることを確認し、Enterを押します。



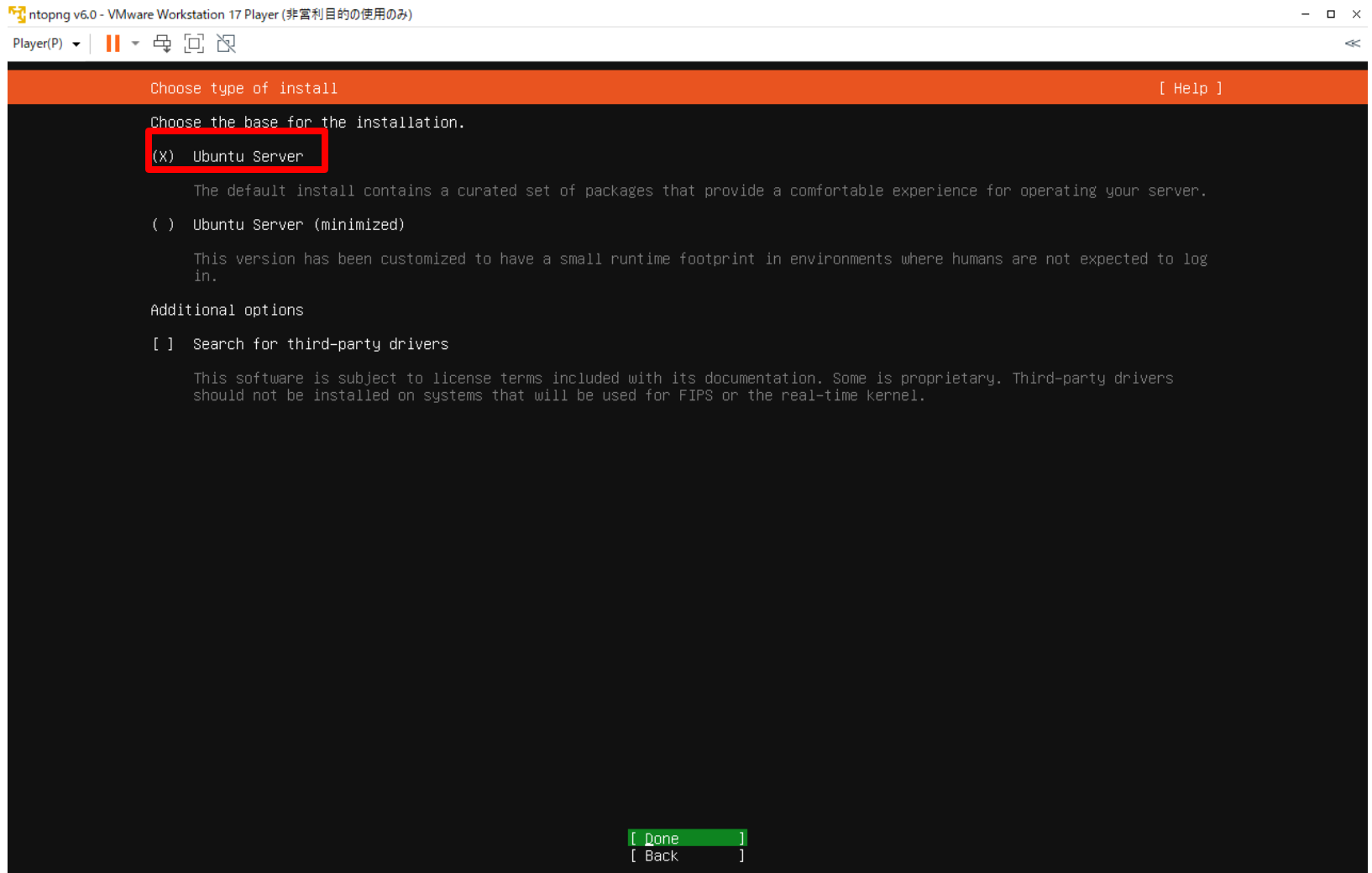
言語選択で「English」が選択されていることを確認し、Enterを押します。



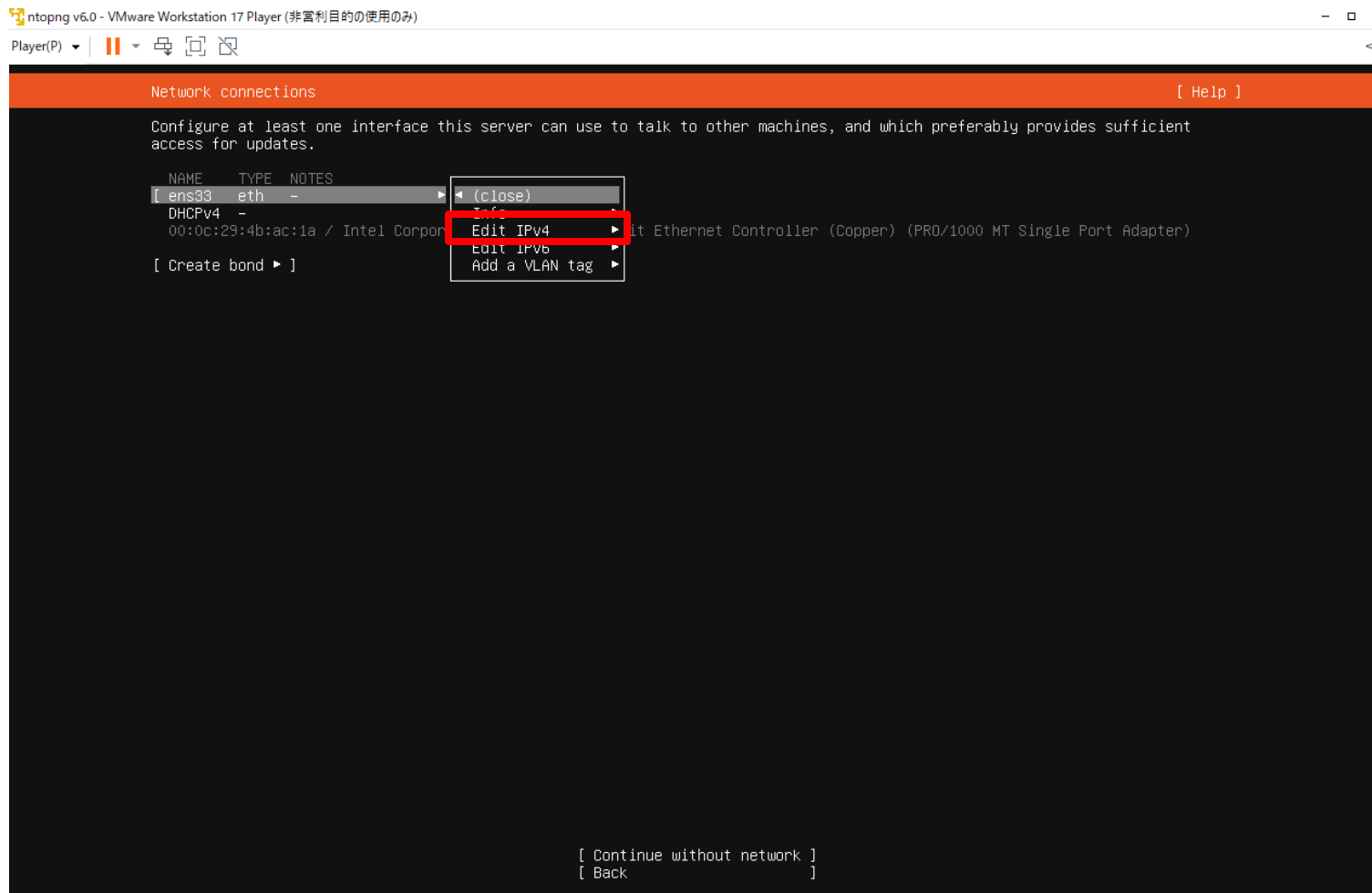
キーボード選択で「Japanese」を選択し、Enterを押します。



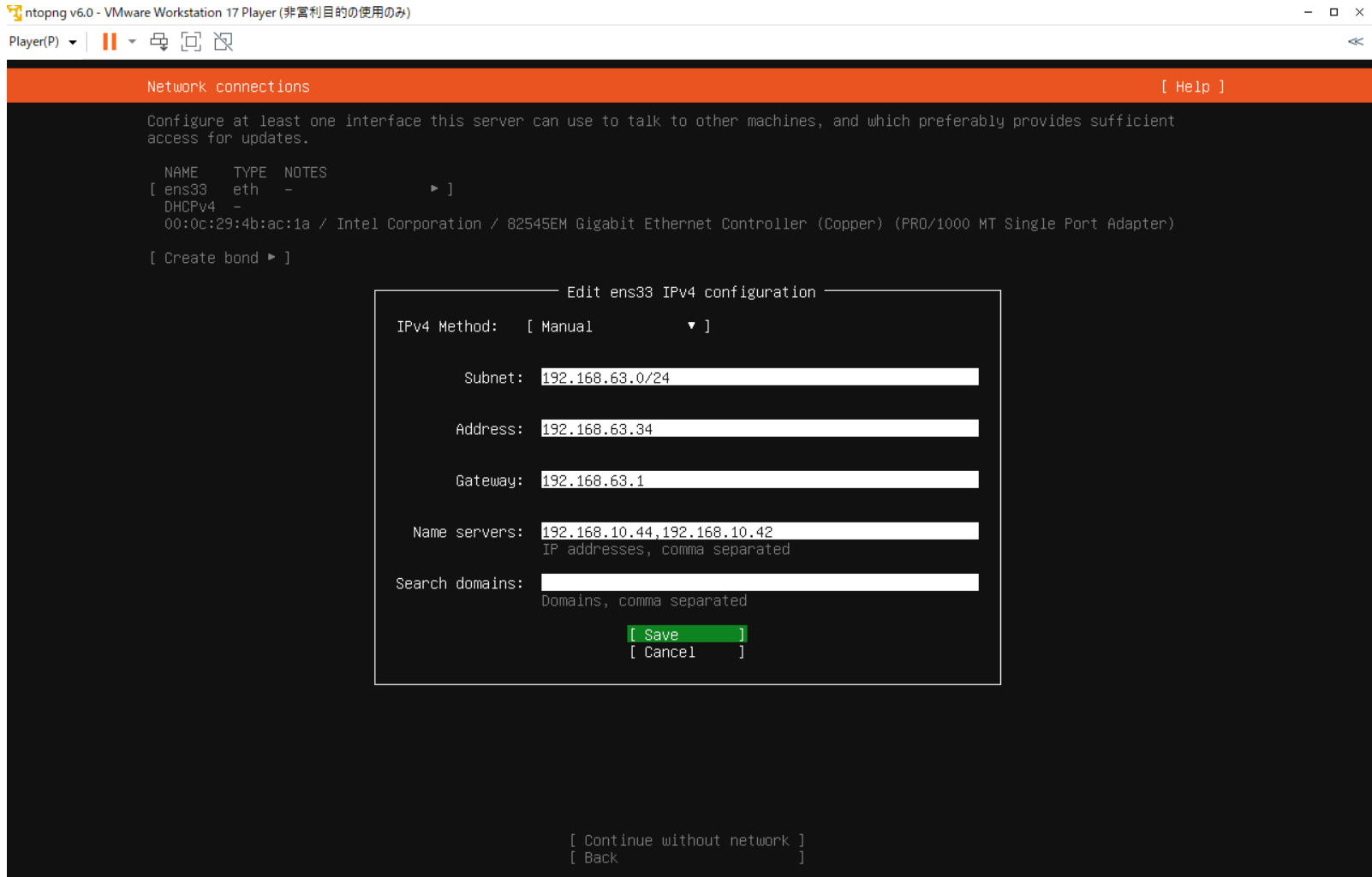
「Ubuntu Server」が選択されていることを確認し、「Done」を選択Enterを押します。



環境によいIPアドレスを設定してください。以下は手動でIPアドレスを設定する例です。該当のNICを選択し、「Edit IPv4」を選択し、Enterをクリックします。



IPアドレスを設定してください。以下は手動でIPアドレスを設定する例です。



The screenshot shows the ntopng v6.0 network configuration interface. At the top, it says "Network connections" and "[Help]". Below that, it instructs to "Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient access for updates." A table lists network interfaces:

NAME	TYPE	NOTES
[ens33	eth	-

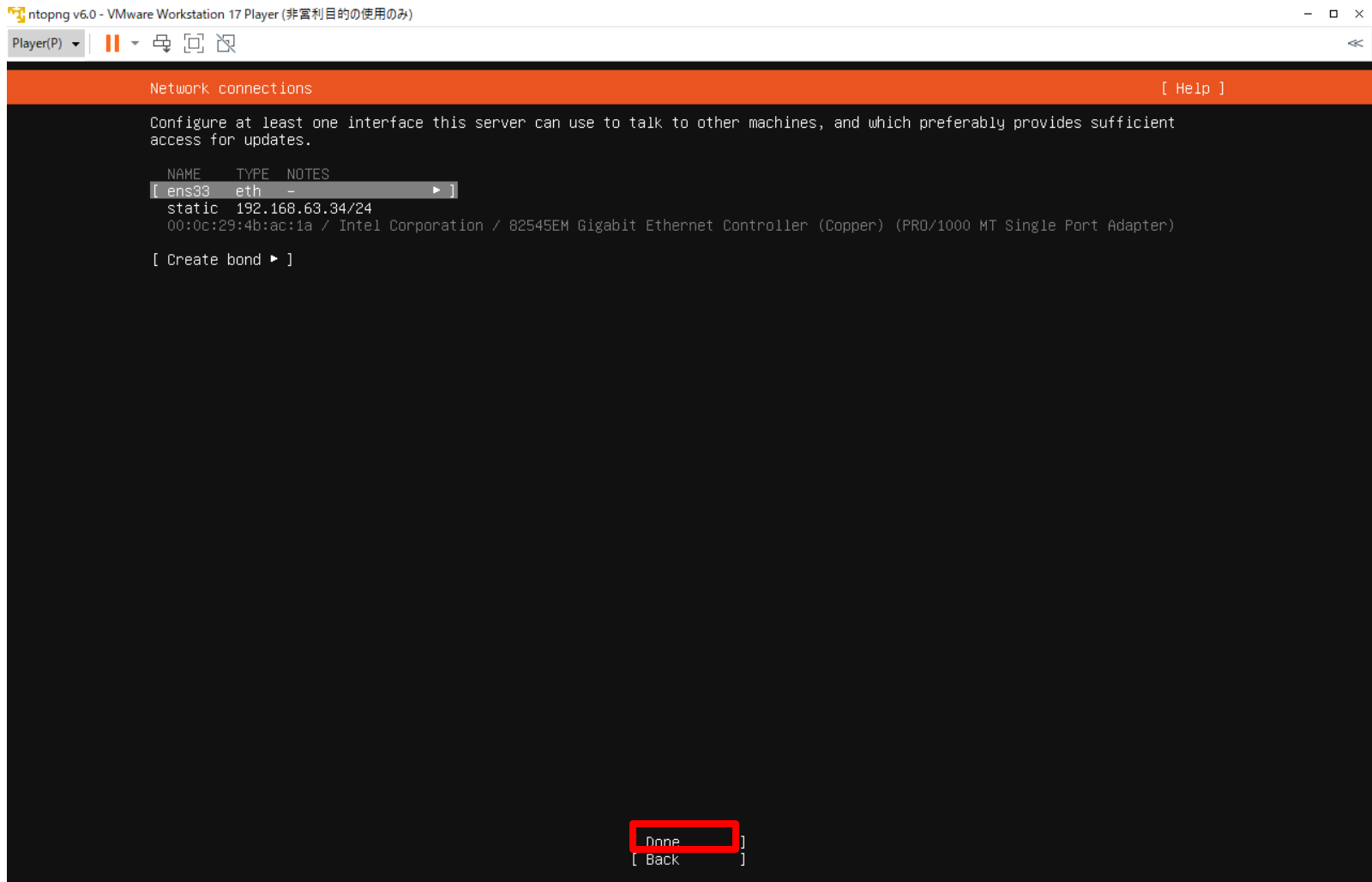
Below the table, it shows "DHCPv4 -" and "00:0c:29:4b:ac:1a / Intel Corporation / 82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)". There is a "[Create bond ▶]" option.

The main part of the dialog is titled "Edit ens33 IPv4 configuration". It has the following fields:

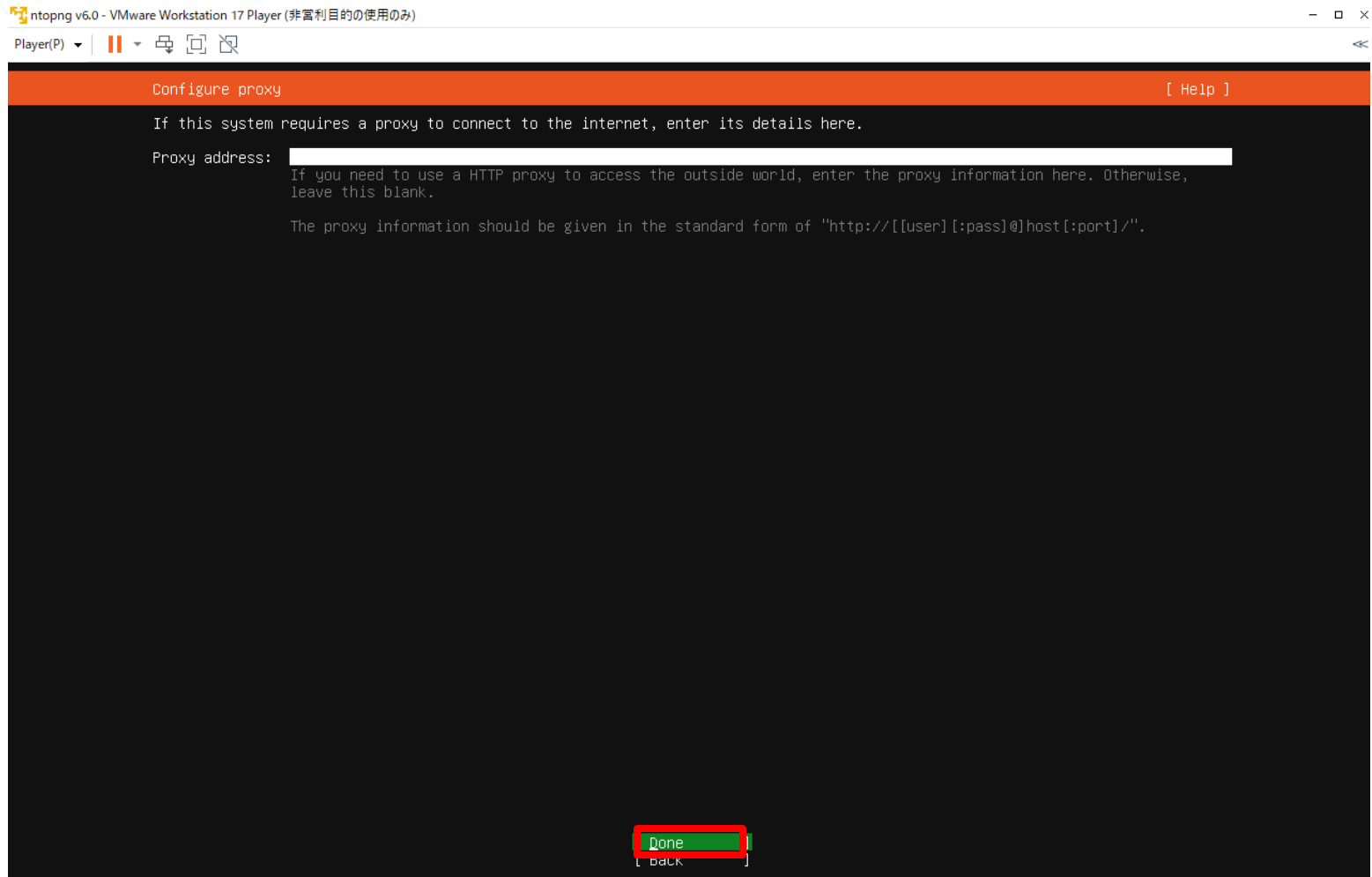
- IPv4 Method: [Manual ▼]
- Subnet: 192.168.63.0/24
- Address: 192.168.63.34
- Gateway: 192.168.63.1
- Name servers: 192.168.10.44,192.168.10.42
IP addresses, comma separated
- Search domains: [empty]
Domains, comma separated

At the bottom, there are buttons: [Save] (highlighted in green), [Cancel], [Continue without network], and [Back].

設定が完了したら、「Done」を選択しEnterを押します。



プロキシ環境でなければ、「Done」を選択しEnterを押します。



「Done」を選択しEnterを押します。

ntopng v6.0 - VMware Workstation 17 Player (非営利目的の使用のみ)

Player(P) | || | | | |

```
Configure Ubuntu archive mirror [ Help ]

If you use an alternative mirror for Ubuntu, enter its details here.

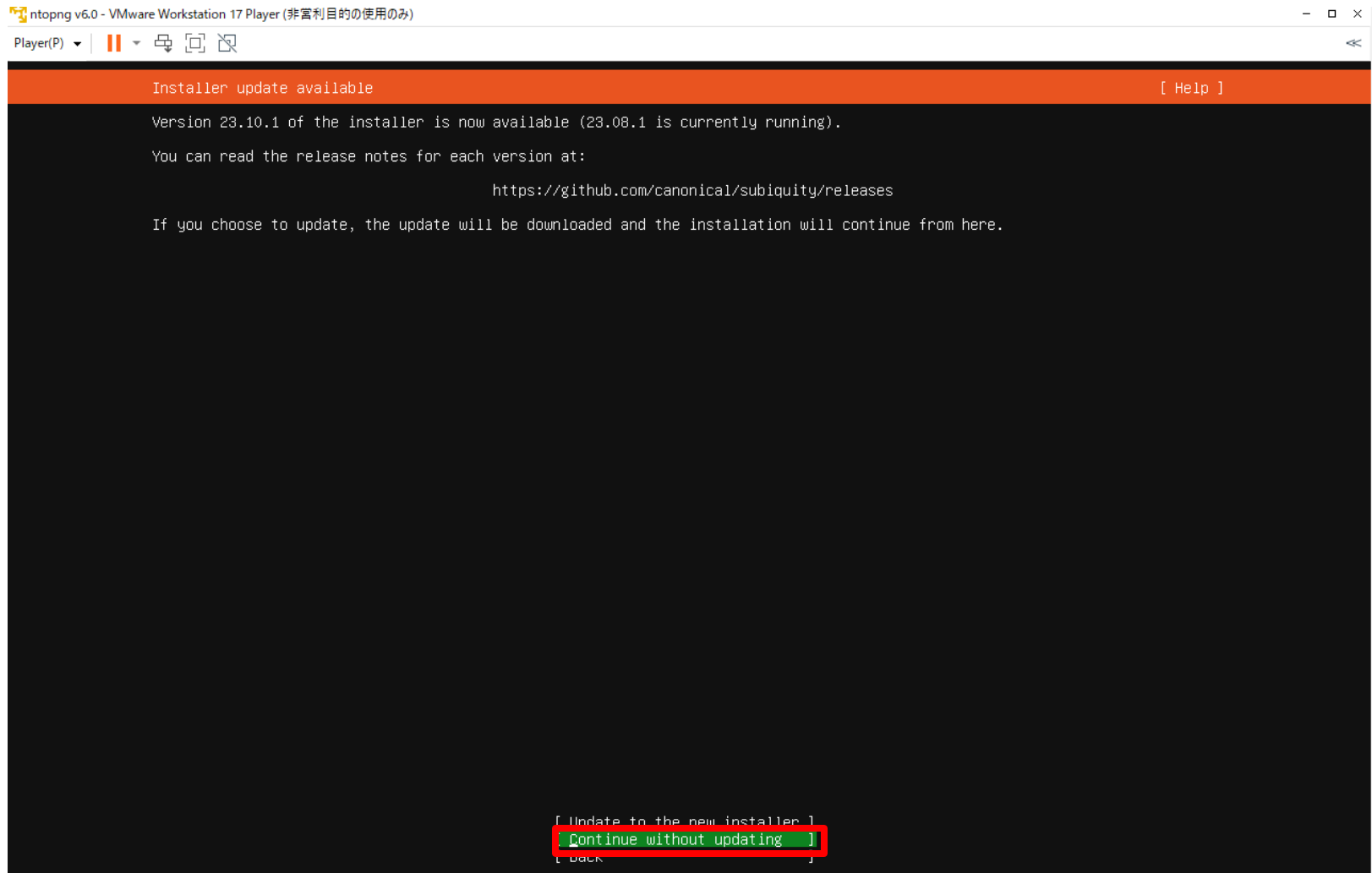
Mirror address: http://jp.archive.ubuntu.com/ubuntu
                You may provide an archive mirror that will be used instead of the default.

The mirror location is being tested. \

Hit:1 http://jp.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://jp.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://jp.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]

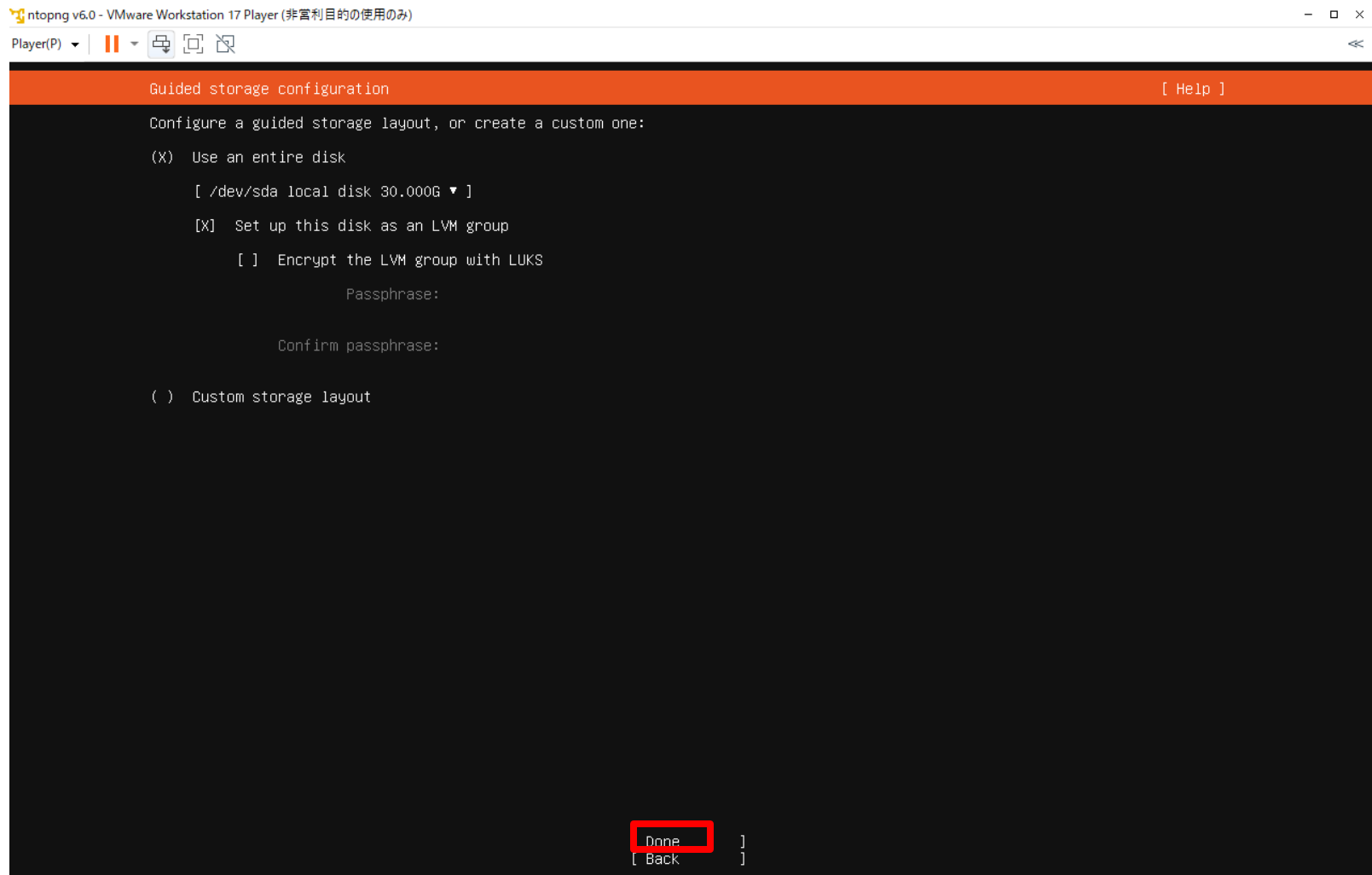
Done
[ Back ]
```

「Continue without updating」を選択しEnterを押します。

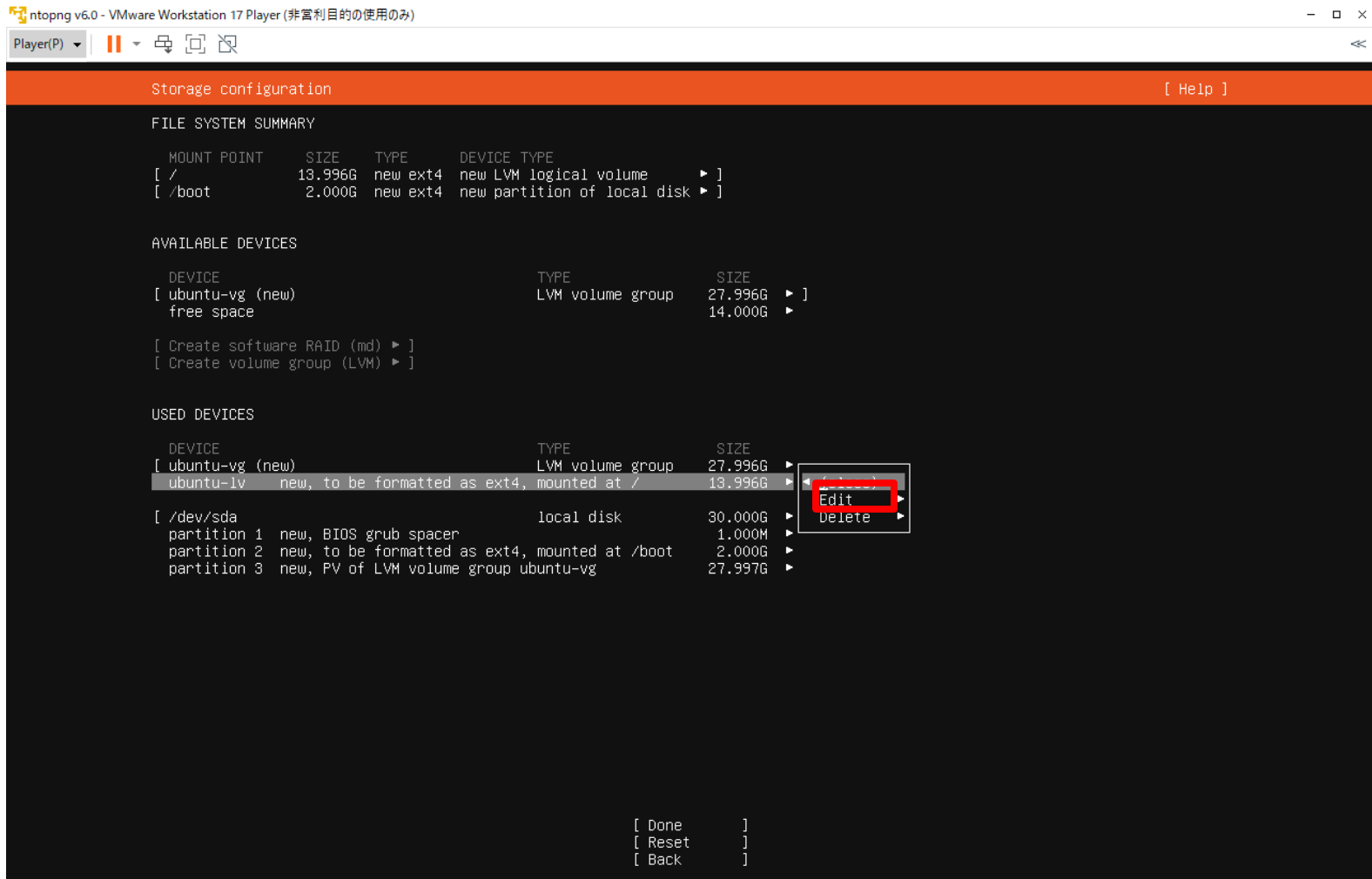


```
ntopng v6.0 - VMware Workstation 17 Player (非営利目的の使用のみ)
Player(P) | || | | |
Installer update available [ Help ]
Version 23.10.1 of the installer is now available (23.08.1 is currently running).
You can read the release notes for each version at:
https://github.com/canonical/subiquity/releases
If you choose to update, the update will be downloaded and the installation will continue from here.
[ Update to the new installer ]
[ Continue without updating ]
[ Back ]
```

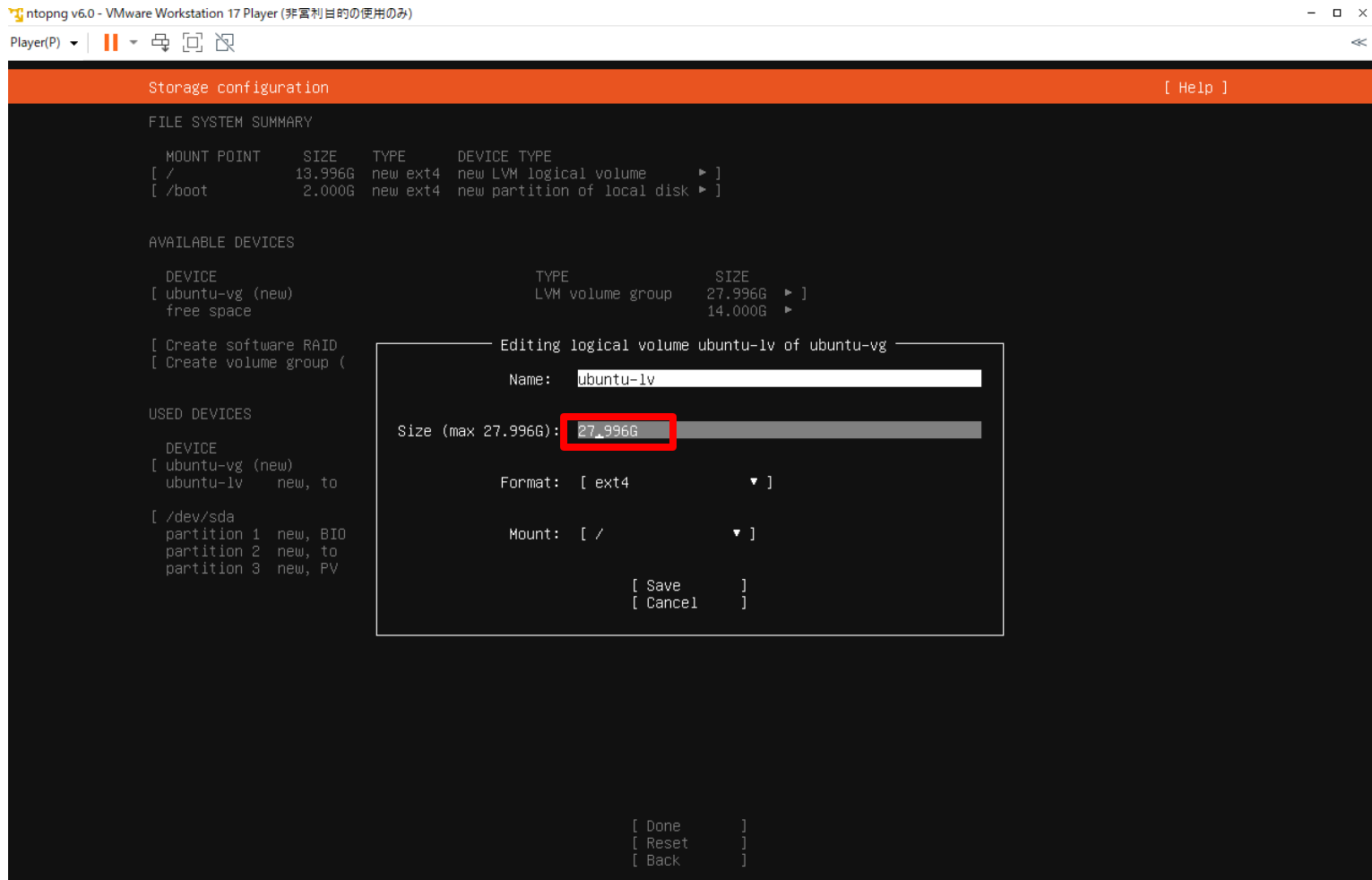
「Done」を選択しEnterを押します。



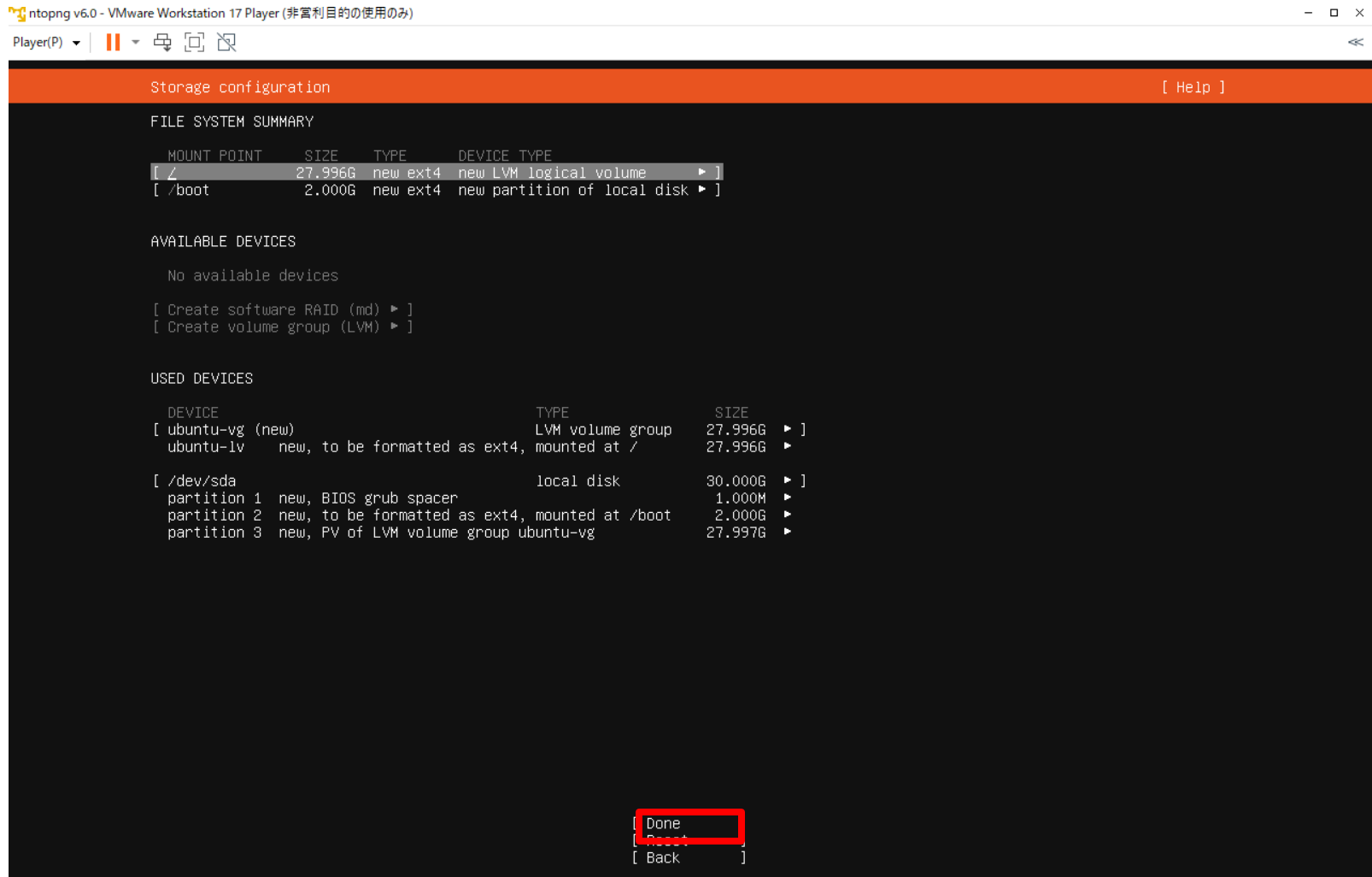
「ubuntu-lv」を選択しEnterを押します。「Edit」を選択し、Enterを押します。



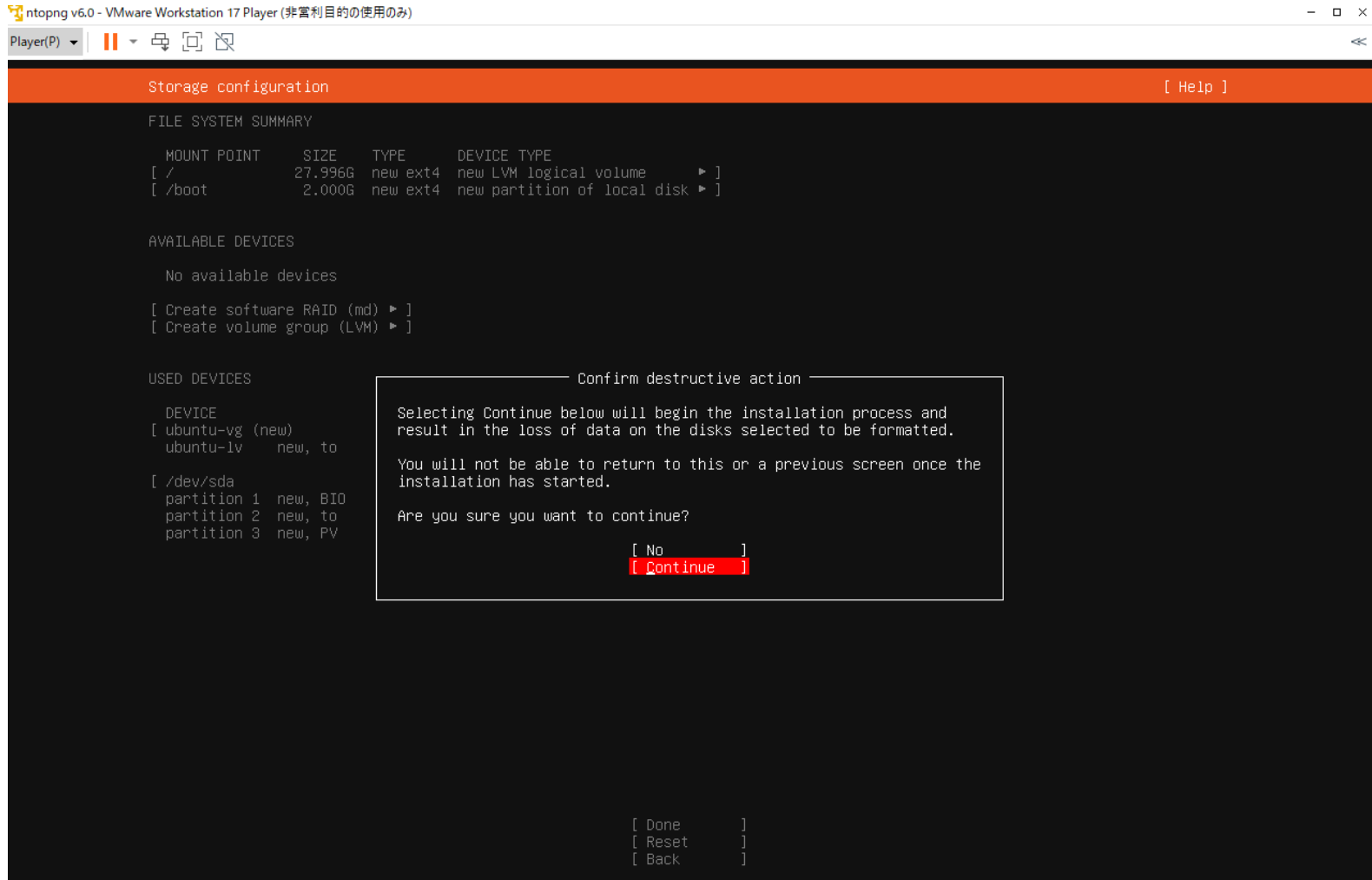
「Size」に最大サイズを設定。「Save」を選択し、Enterを押します。



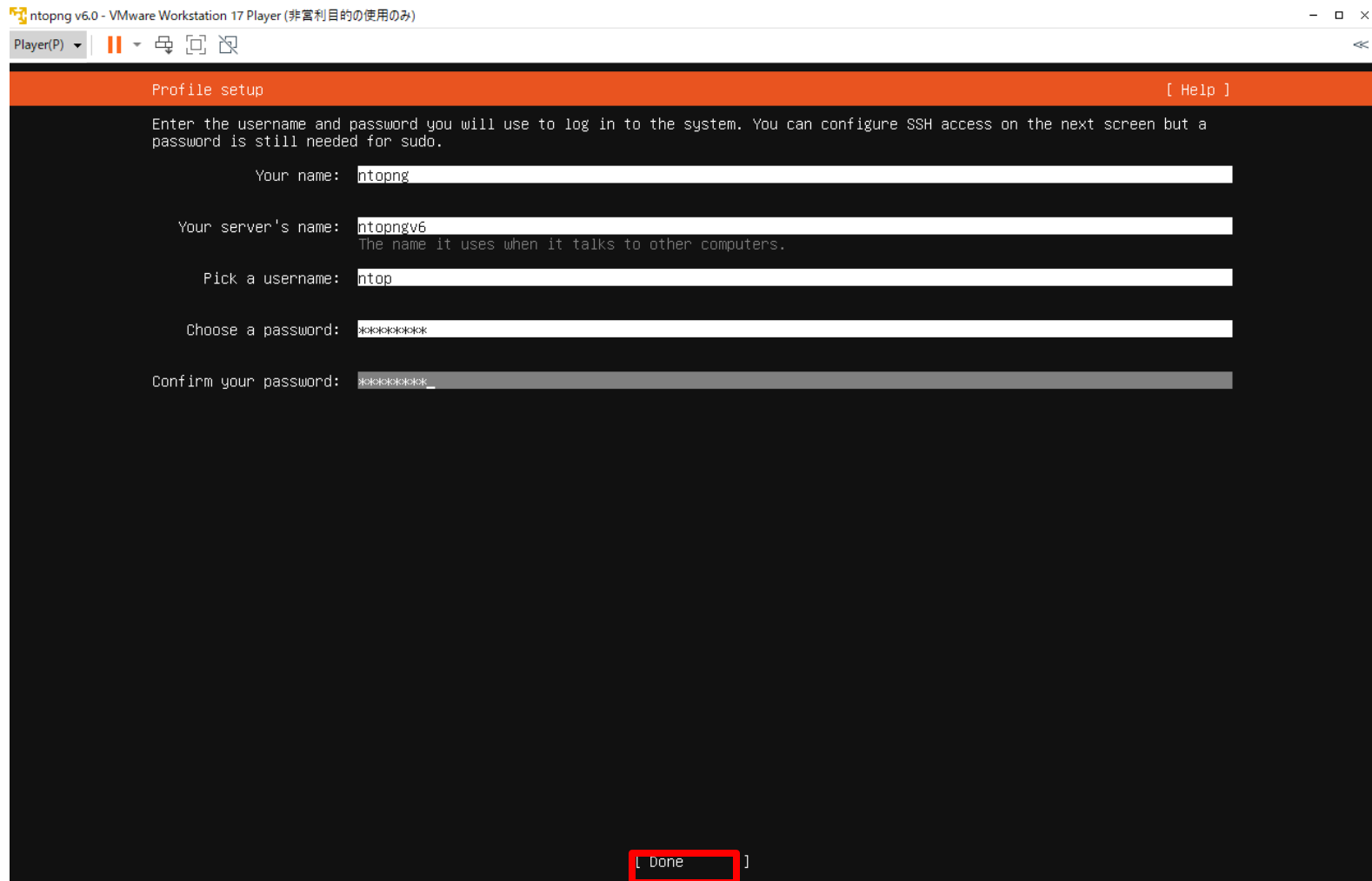
「Done」を選択し、Enterを押します。



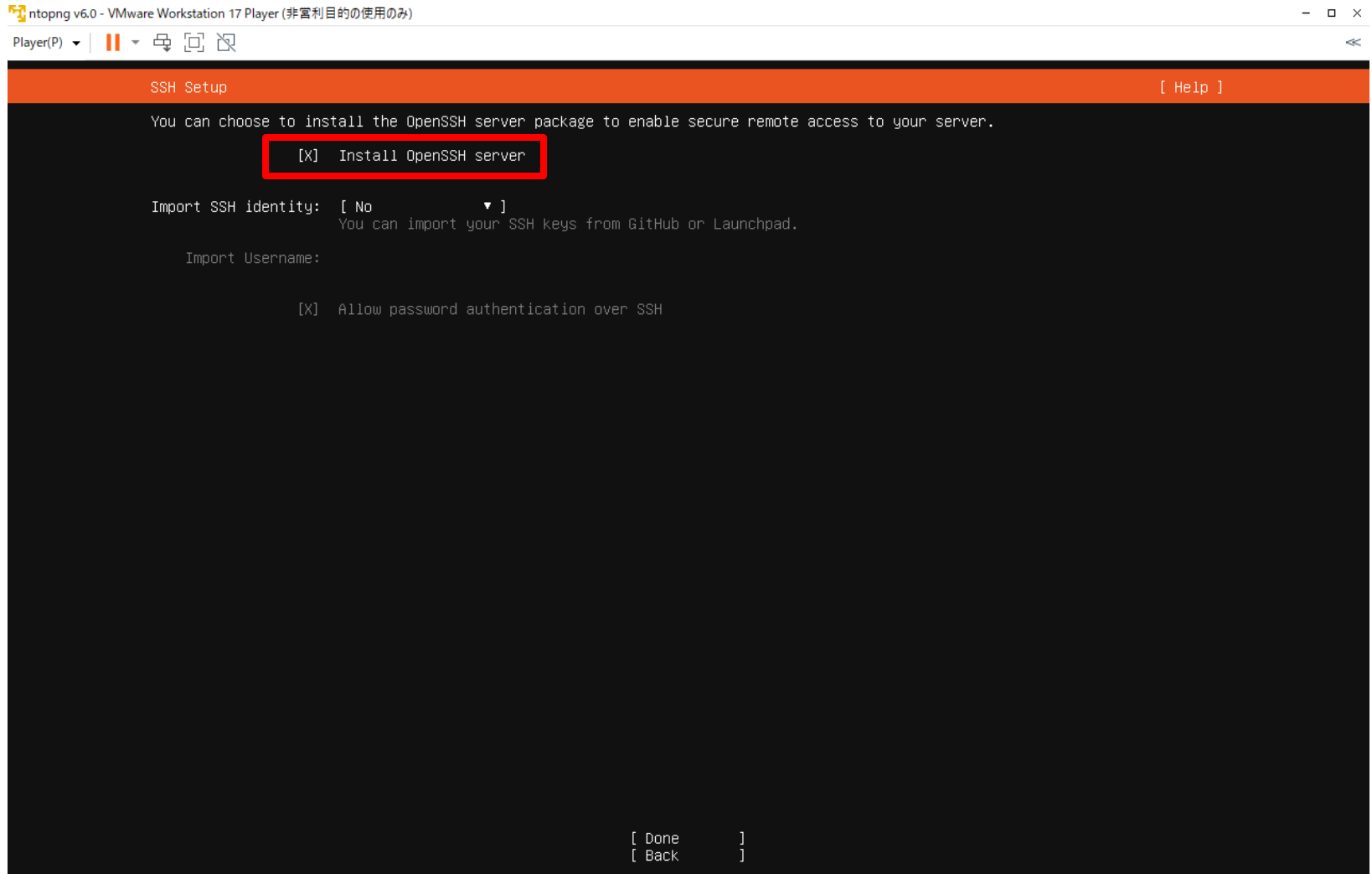
「Continue」を選択し、Enterを押します。



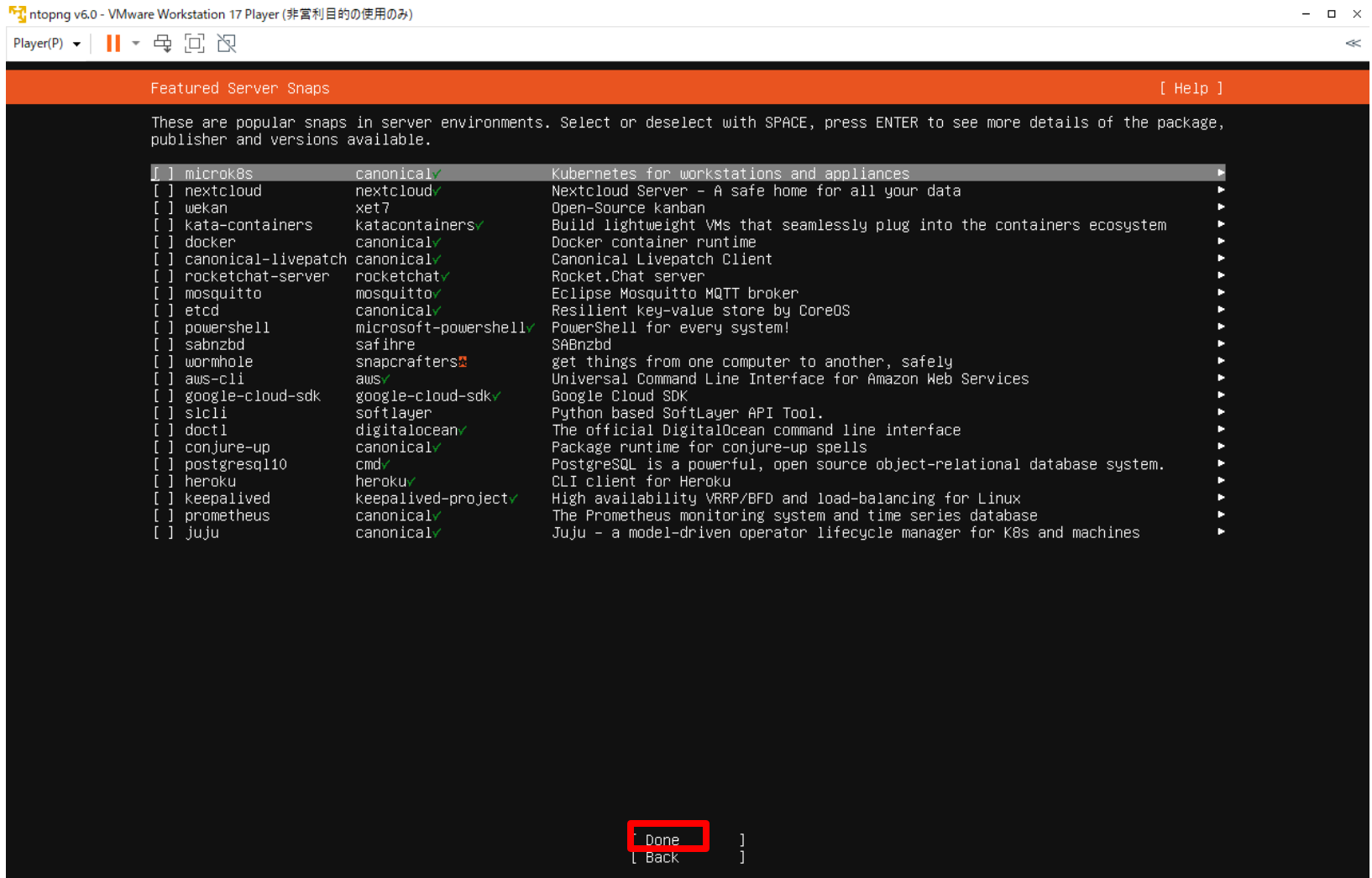
サーバー名、ユーザー名を設定し、「Done」を選択しEnterを押します。



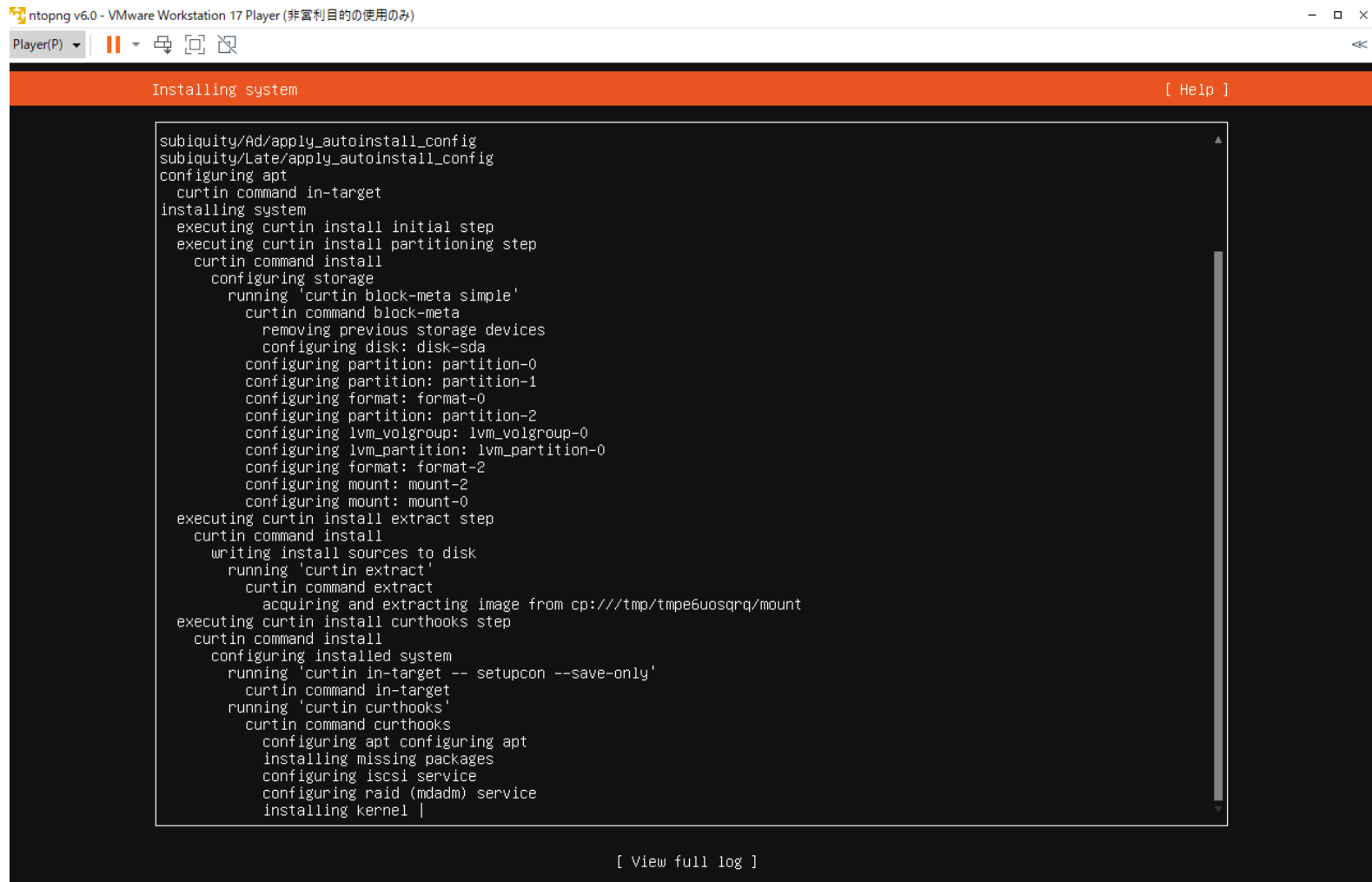
「Install OpenSSH server」に✓を入れ、「Done」を選択しEnterを押します。



「Done」を選択しEnterを押します。



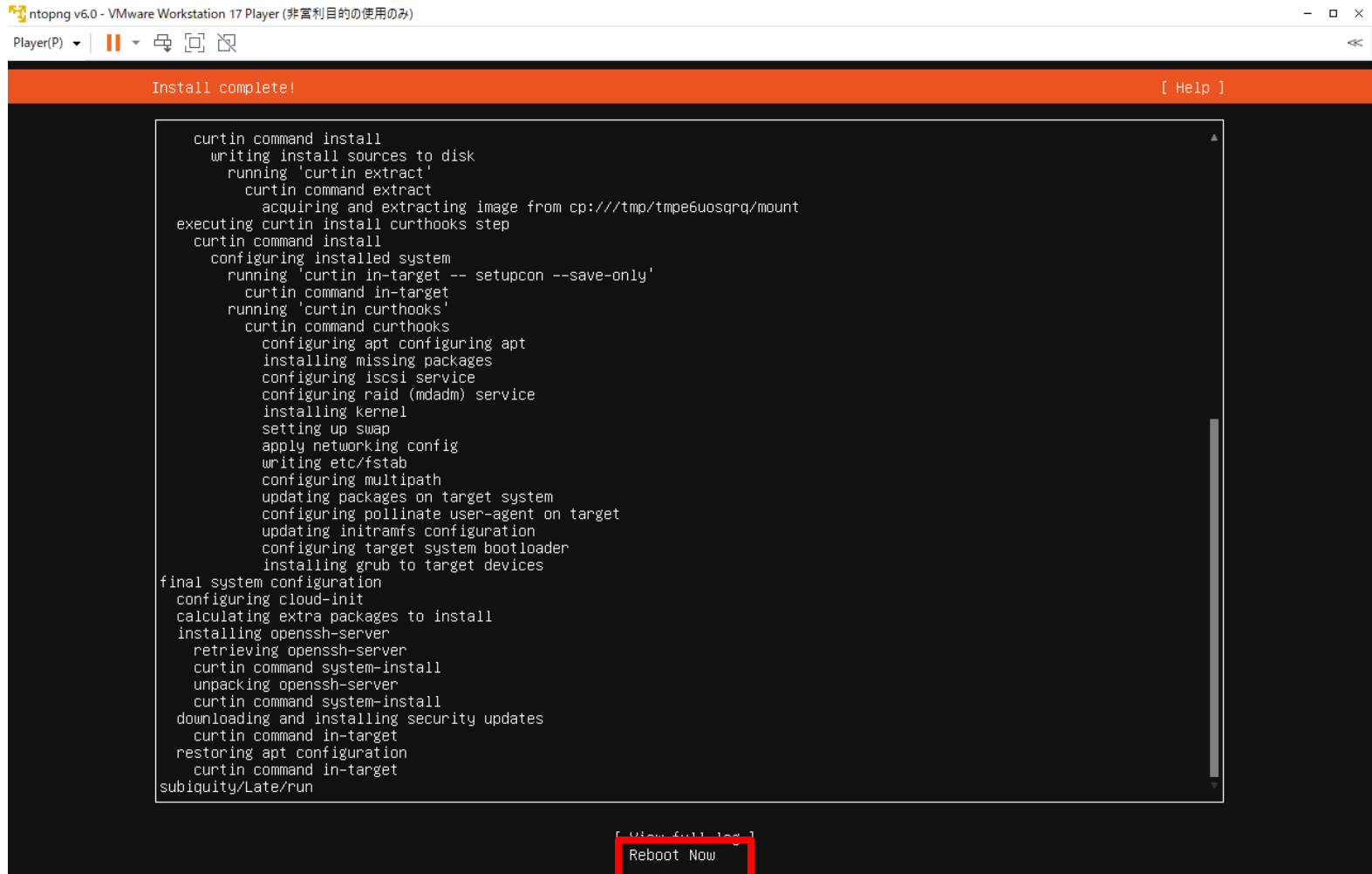
インストールが開始します。しばらくお待ちください。



```
ntopng v6.0 - VMware Workstation 17 Player (非営利目的の使用のみ)
Player(P) [ Paused ] [ Full Screen ] [ Refresh ] [ Close ]
Installing system [ Help ]
subiquity/Ad/apply_autoinstall_config
subiquity/Late/apply_autoinstall_config
configuring apt
  curtin command in-target
installing system
  executing curtin install initial step
  executing curtin install partitioning step
    curtin command install
    configuring storage
      running 'curtin block-meta simple'
      curtin command block-meta
        removing previous storage devices
        configuring disk: disk-sda
        configuring partition: partition-0
        configuring partition: partition-1
        configuring format: format-0
        configuring partition: partition-2
        configuring lvm_volgroup: lvm_volgroup-0
        configuring lvm_partition: lvm_partition-0
        configuring format: format-2
        configuring mount: mount-2
        configuring mount: mount-0
    executing curtin install extract step
    curtin command install
      writing install sources to disk
      running 'curtin extract'
      curtin command extract
        acquiring and extracting image from cp:///tmp/tmp6u0sqrq/mount
    executing curtin install curthooks step
    curtin command install
      configuring installed system
      running 'curtin in-target -- setupcon --save-only'
      curtin command in-target
      running 'curtin curthooks'
      curtin command curthooks
        configuring apt configuring apt
        installing missing packages
        configuring iscsi service
        configuring raid (mdadm) service
        installing kernel |

[ View full log ]
```

「Install complete!」と表示されたのちに、「Reboot Now」を選択しEnterを押します。これでインストールは完了です。



4. ntopngのインストール

本章では以下のバージョンを使用しています。

- ◆ Windows 11 x64
 - ◆ nProbe 10.X and ntopng v6.X Stable版
 - ◆ VMware Workstation 17
-

前章でISOからインストールしたubuntuサーバーには、ntopngのインストールスクリプトが包含されております。本章では、インストールスクリプトを実行しntopngをインストールします。

前章でインストールしたubuntuにログインしてください。そして、/homeに移動しインストールスクリプトを実行します。実行ユーザーはインストール時に作成したユーザーで、sudoを使います。

```
$cd /home  
$sudo bash -x ntopng_v6_install.sh
```




ntopngのインストール(2)

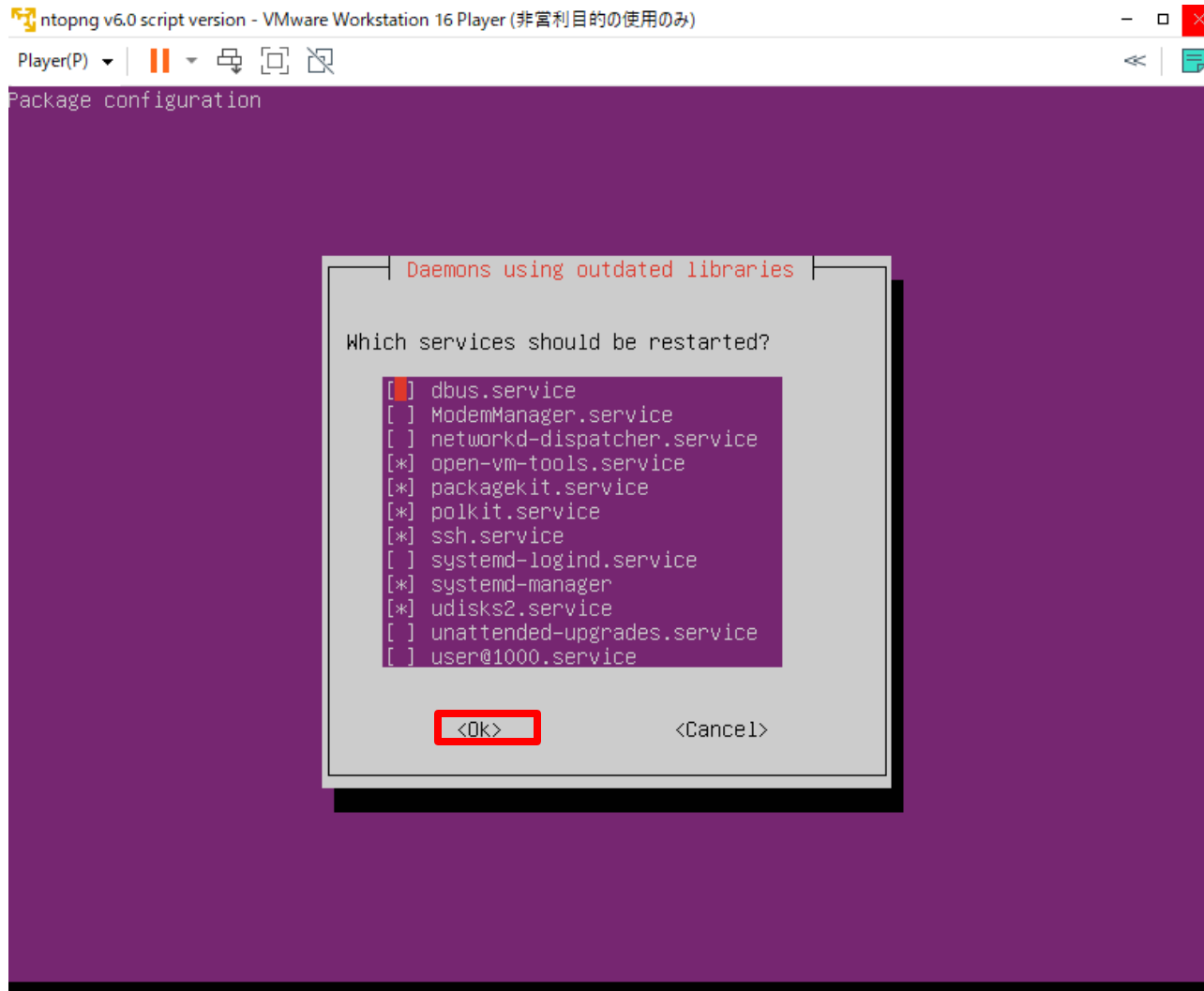
「Do you want to continue? [Y/n]」と表示されるので、「Y」を入力しEnterを押します。

```
ntopng v6.0 script version - VMware Workstation 16 Player (非営利目的の使用のみ)
Player(P) | [Icons] | [Close]
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ntop@ntopngv6:~$ ls
ntop@ntopngv6:~$ cd /home/
ntop@ntopngv6:/home$ ls
ntop ntopng_v6_install.sh
ntop@ntopngv6:/home$ sudo bash -x ntopng_v6_install.sh
[sudo] password for ntop:
+ sudo apt-get update
Hit:1 http://jp.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://jp.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://jp.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://jp.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
+ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  python3-update-manager ubuntu-advantage-tools update-manager-core
The following packages will be upgraded:
  apparmor apt apt-utils bind9-dnsutils bind9-host bind9-libs cloud-init cryptsetup cryptsetup-bin
  cryptsetup-initramfs distro-info-data git git-man initramfs-tools initramfs-tools-bin
  initramfs-tools-core irqbalance kpartx libapparmor1 libapt-pkg6.0 libcryptsetup12 libldap-2.5-0
  libldap-common libnetplan0 libnss-systemd libpam-systemd libsgutils2-2 libsystemd0 libudev1
  multipath-tools netplan.io python3-software-properties sg3-utils sg3-utils-udev
  software-properties-common sosreport systemd systemd-hwe-hwdb systemd-sysv systemd-timesyncd
  ubuntu-drivers-common udev
42 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Need to get 19.0 MB of archives.
After this operation, 5,853 kB disk space will be freed.
Do you want to continue? [Y/n]
```

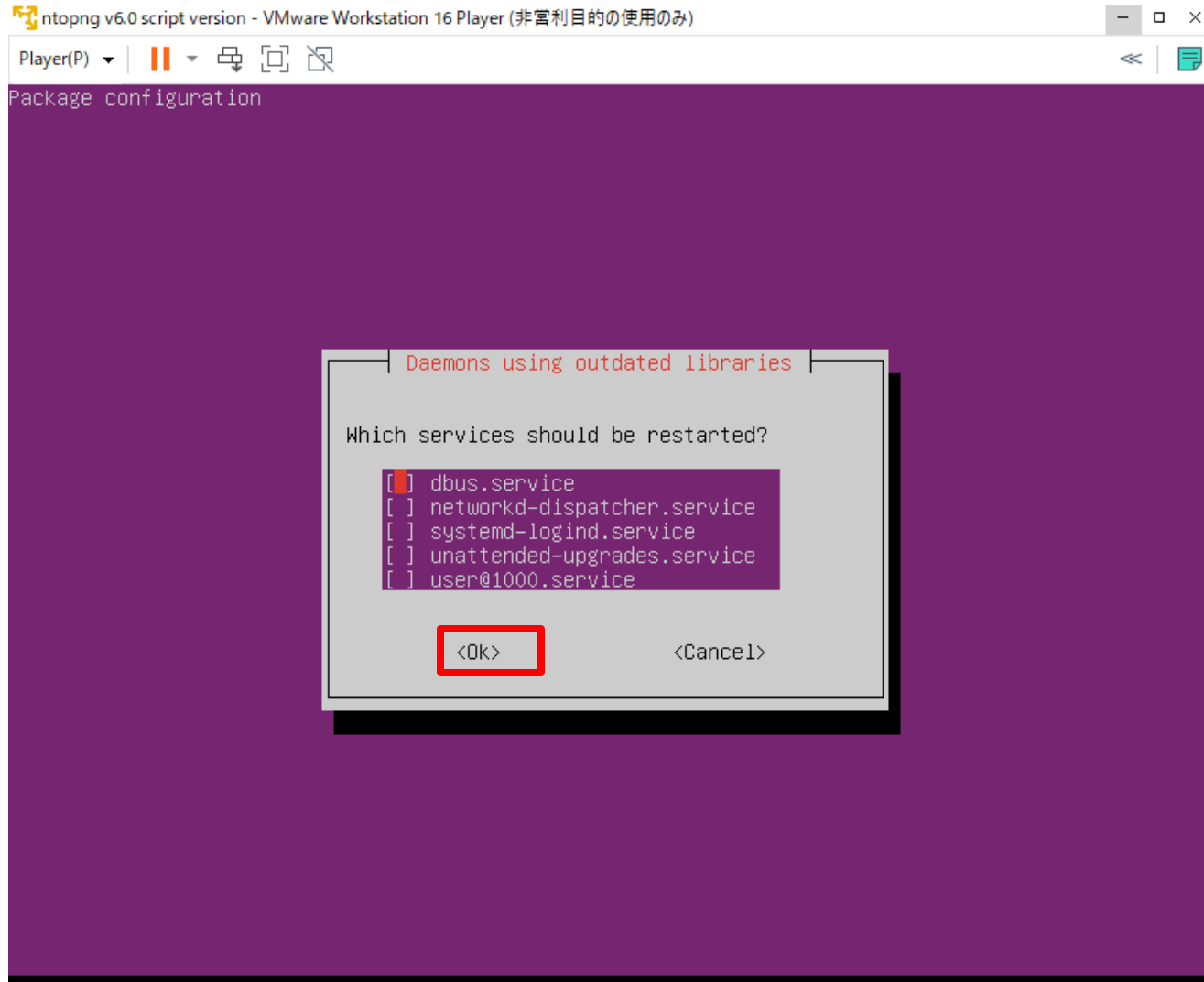
下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



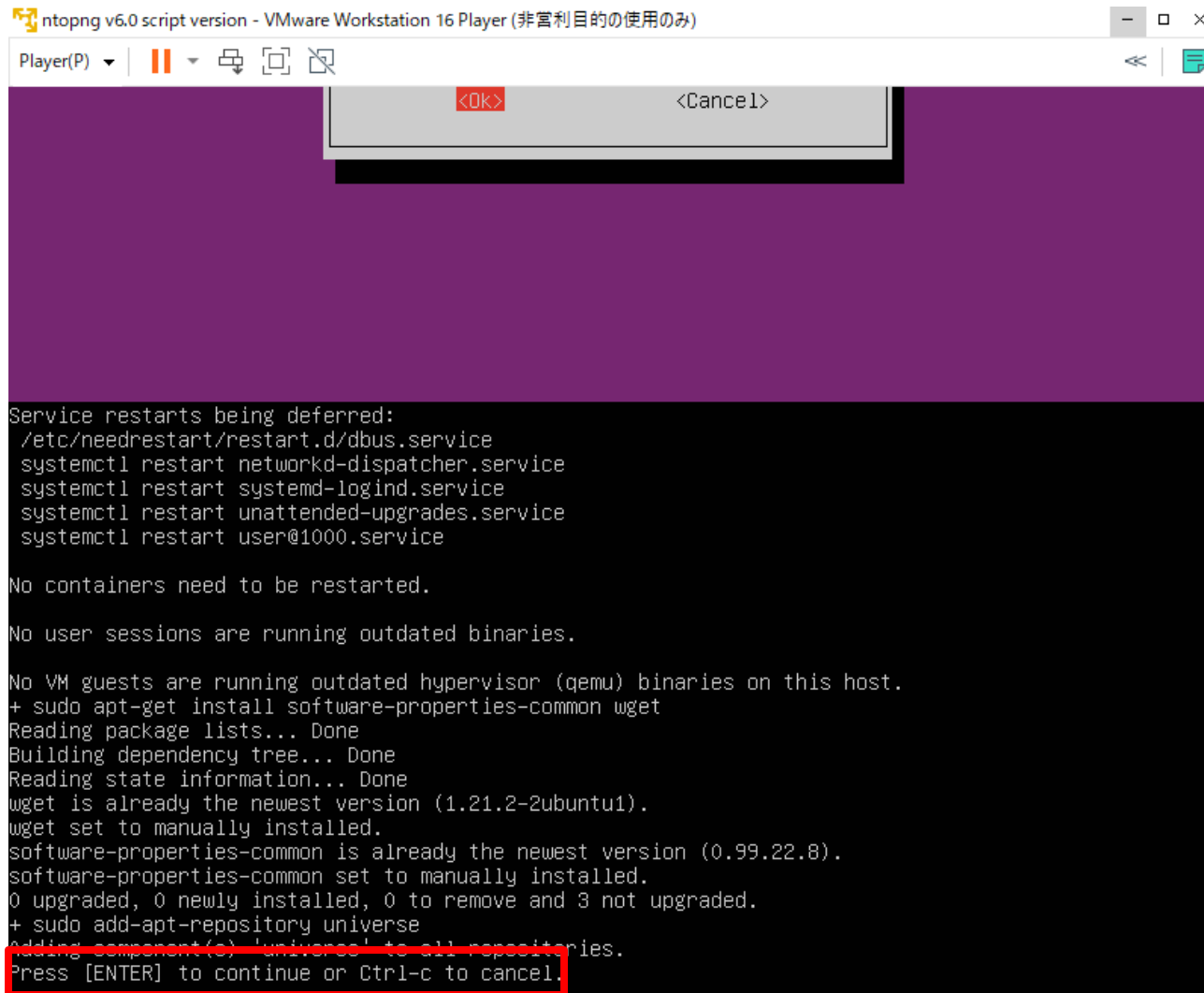
「Enter Password for default user:」と表示されるので、**必ず”default”と入力しEnterを押します**

```
ntopng v6.0 script version - VMware Workstation 16 Player (非営利目的の使用のみ)
Player(P) | [Icons] | [Close]
Creating symlink /usr/bin/clickhouse-extract-from-config to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-keeper already exists but it points to /clickhouse. Will replace the old
symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-keeper to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-keeper-converter already exists but it points to /clickhouse. Will repla
ce the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-keeper-converter to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-disks to /usr/bin/clickhouse.
Creating symlink /usr/bin/ch to /usr/bin/clickhouse.
Creating symlink /usr/bin/ch1 to /usr/bin/clickhouse.
Creating symlink /usr/bin/chc to /usr/bin/clickhouse.
Creating clickhouse group if it does not exist.
groupadd -r clickhouse
Creating clickhouse user if it does not exist.
useradd -r --shell /bin/false --home-dir /nonexistent -g clickhouse clickhouse
Will set ulimits for clickhouse user in /etc/security/limits.d/clickhouse.conf.
Creating config directory /etc/clickhouse-server/config.d that is used for tweaks of main server con
figuration.
Creating config directory /etc/clickhouse-server/users.d that is used for tweaks of users configurat
ion.
Config file /etc/clickhouse-server/config.xml already exists, will keep it and extract path info fro
m it.
/etc/clickhouse-server/config.xml has /var/lib/clickhouse/ as data path.
/etc/clickhouse-server/config.xml has /var/log/clickhouse-server/ as log path.
Users config file /etc/clickhouse-server/users.xml already exists, will keep it and extract users in
fo from it.
Creating log directory /var/log/clickhouse-server/.
Creating data directory /var/lib/clickhouse/.
Creating pid directory /var/run/clickhouse-server.
chown -R clickhouse:clickhouse '/var/log/clickhouse-server/'
chown -R clickhouse:clickhouse '/var/run/clickhouse-server'
chown clickhouse:clickhouse '/var/lib/clickhouse/'
groupadd -r clickhouse-bridge
useradd -r --shell /bin/false --home-dir /nonexistent -g clickhouse-bridge clickhouse-bridge
chown -R clickhouse-bridge:clickhouse-bridge '/usr/bin/clickhouse-odbc-bridge'
chown -R clickhouse-bridge:clickhouse-bridge '/usr/bin/clickhouse-library-bridge'
Enter password for default user:
```

下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



「Press [ENTER] to continue …」と表示されるので、Enterを押します。



```
ntopng v6.0 script version - VMware Workstation 16 Player (非営利目的の使用のみ)
Player(P) | || | | |
<Ok> <Cancel>

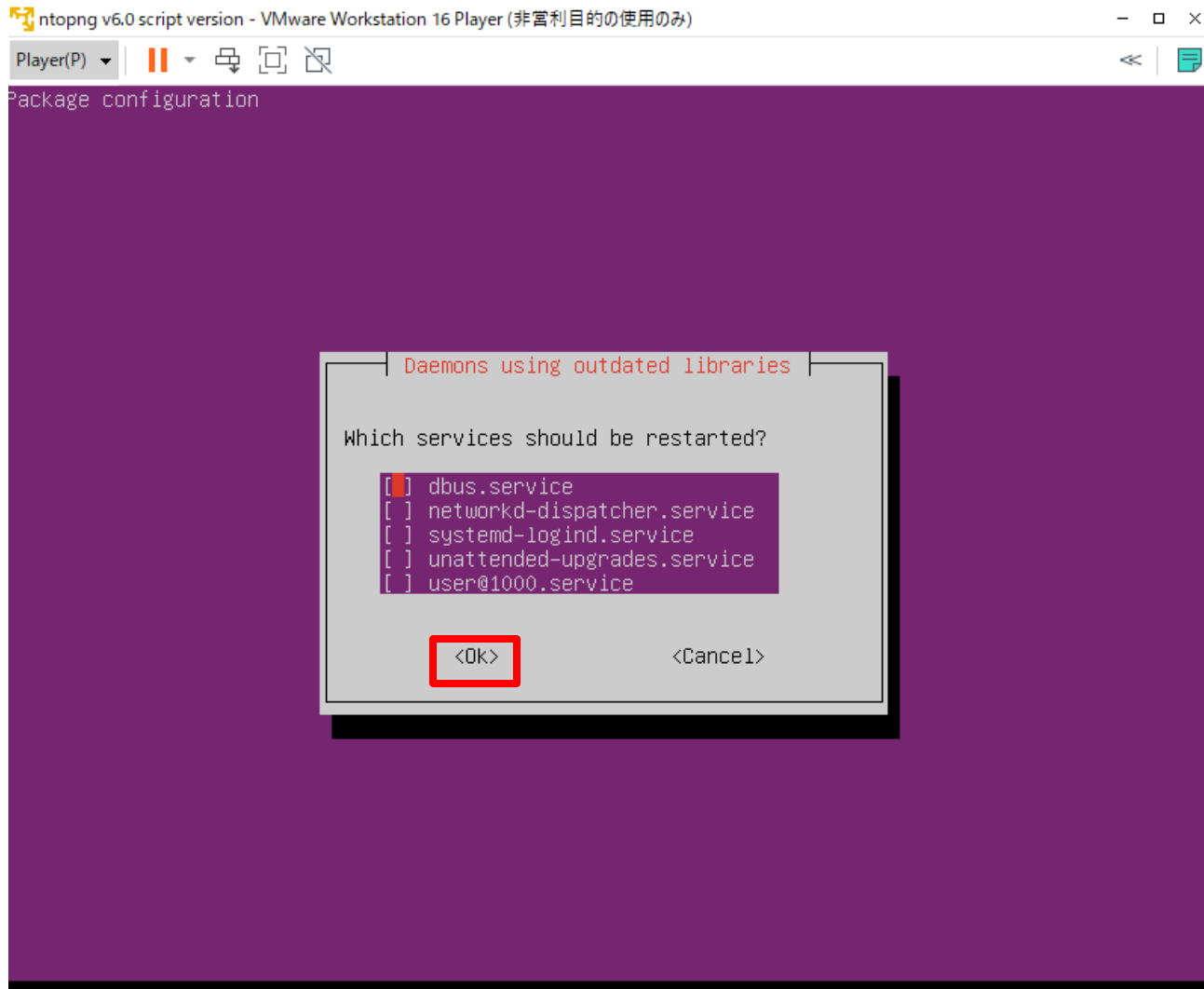
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart networkd-dispatcher.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
+ sudo apt-get install software-properties-common wget
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wget is already the newest version (1.21.2-2ubuntu1).
wget set to manually installed.
software-properties-common is already the newest version (0.99.22.8).
software-properties-common set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
+ sudo add-apt-repository universe
adding component(s) 'universe' to all repositories.
Press [ENTER] to continue or Ctrl-c to cancel.
```

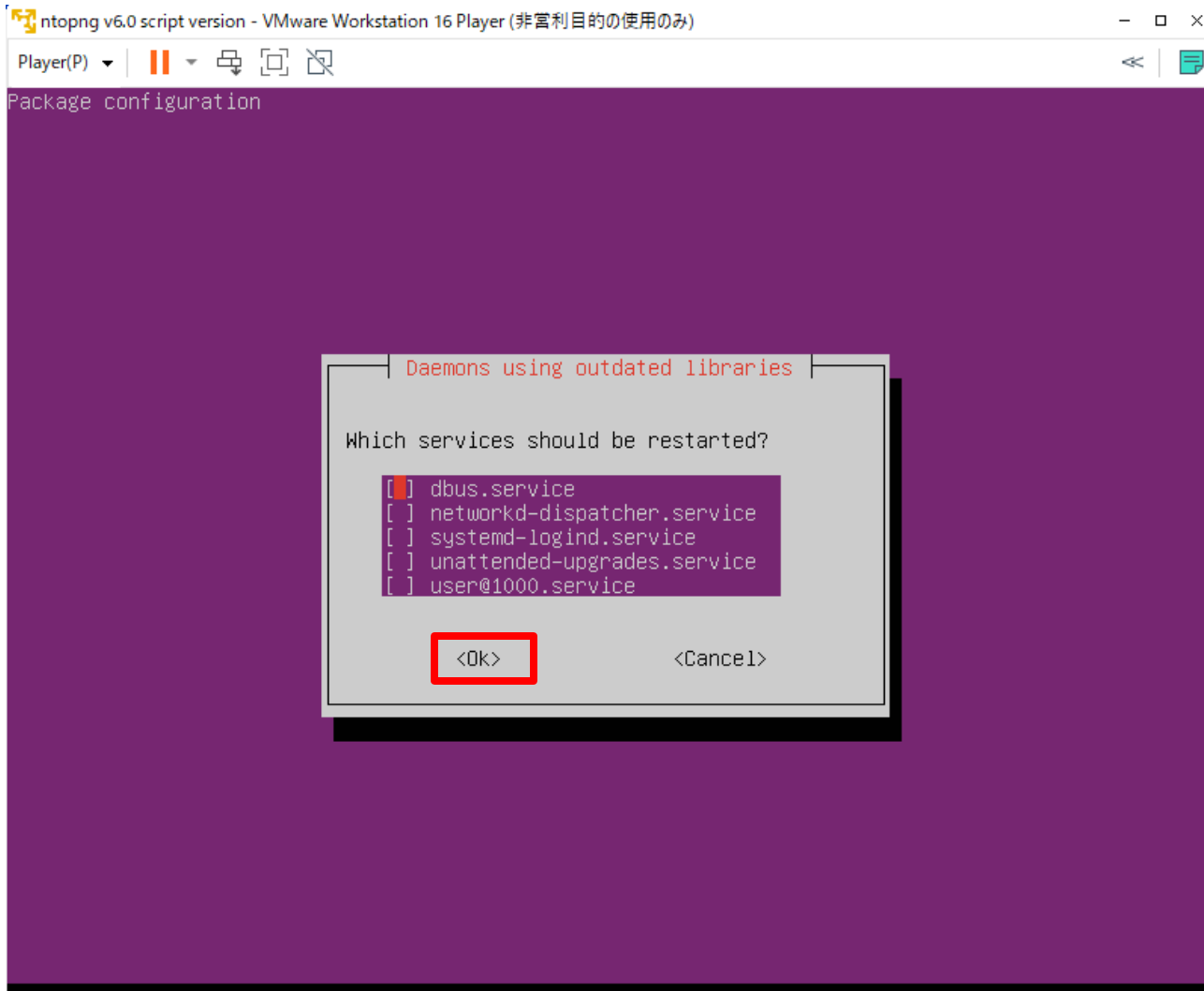
下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



「Do you want to continue?[Y/n]」と表示されるので、「Y」を入力しEnterを押します。

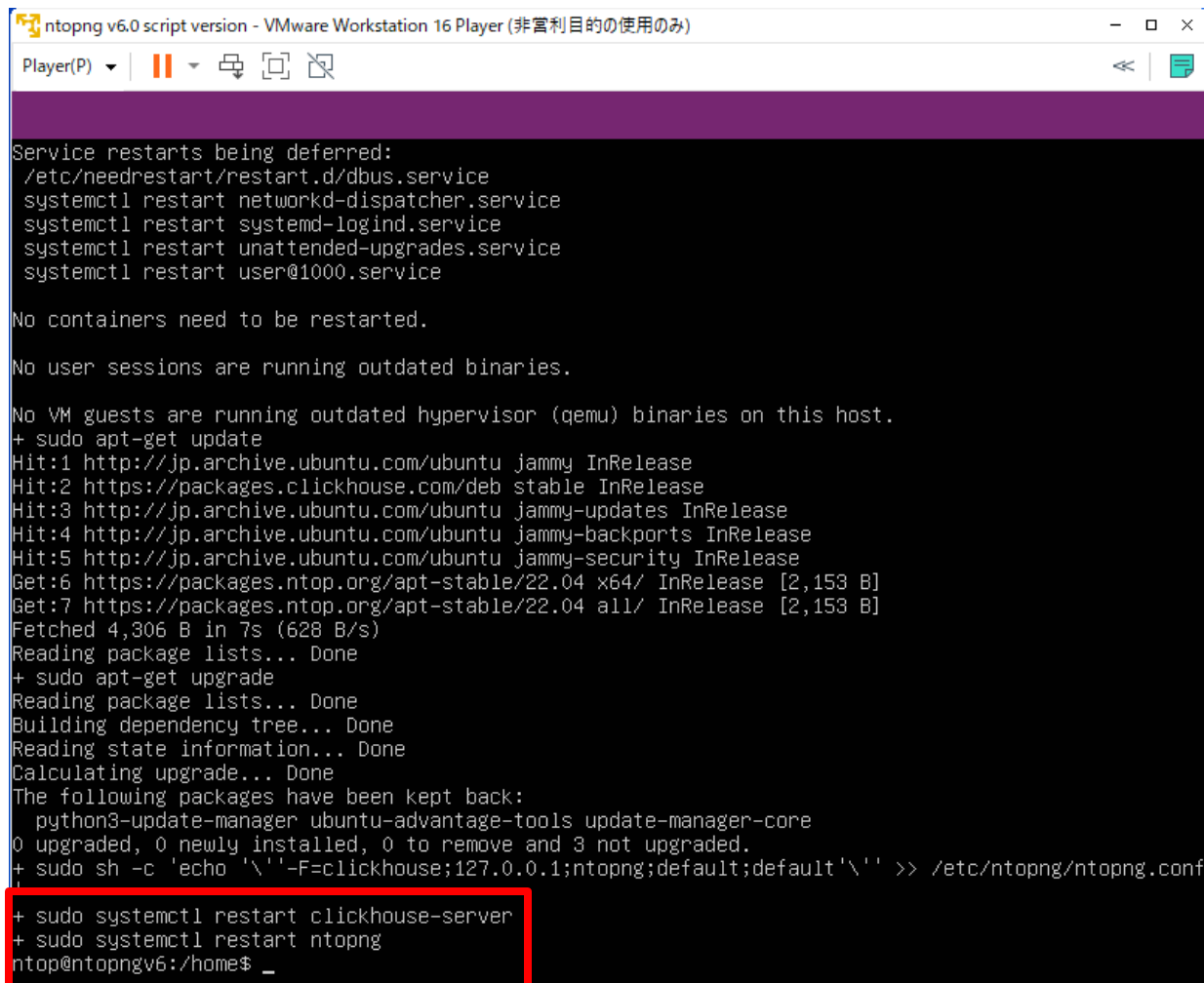
```
ntopng v6.0 script version - VMware Workstation 16 Player (非営利目的の使用のみ)
Player(P) | || | | |
libatomic1 libblas3 libc-dev-bin libc-devtools libc6-dev libcairo2 libcc1-0 libcrypt-dev
libdatrie1 libdbi1 libdeflate0 libdpkg-perl libfakeroot libfile-fcntllock-perl libfontconfig1
libgcc-11-dev libgcc-12-dev libgd3 libgomp1 libgraphite2-3 libharfbuzz0b libhiredis0.14 libis123
libitm1 libjbig0 libjemalloc2 libjpeg-turbo8 libjpeg8 liblinear4 liblsan0 liblua5.1-0
liblua5.3-0 liblzf1 libmariadb3 libmpc3 libmysqlclient21 libnetfilter-queue1 libnorm1 libnsl-dev
libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpgm-5.3-0 libpixman-1-0 libquadmath0
libradcli4 librdkafka1 librrd8 libsensors-config libsensors5 libsnmp-base libsnmp40
libstdc++-11-dev libthai-data libthai0 libtiff5 libtirpc-dev libtsan0 libtsan2 libubsan1
libwebp7 libxcb-render0 libxcb-shm0 libxpm4 libxrender1 libzmq5 linux-libc-dev lto-disabled-list
lua-bitop lua-cjson lua-lpeg make manpages-dev mariadb-common mysql-common ndpi net-tools nmap
nmap-common ntop-license ntopng-data pfring redis-server redis-tools rpcsvc-proto
Suggested packages:
bzip2-doc cpp-doc gcc-11-locales gcc-12-locales cpp-12-doc debtags menu debian-keyring
g++-multilib g++-11-multilib gcc-11-doc gcc-multilib autoconf automake libtool flex bison gdb
gcc-doc gcc-11-multilib gcc-12-multilib gcc-12-doc glibc-doc bzip2 libgd-tools liblinear-tools
liblinear-dev lm-sensors snmp-mibs-downloader libstdc++-11-doc make-doc ncat ndiff zenmap
ruby-redis
The following NEW packages will be installed:
build-essential bzip2 cpp cpp-11 cpp-12 dctrl-tools dkms dpkg-dev fakeroot fontconfig
fontconfig-config fonts-dejavu-core g++ g++-11 gcc gcc-11 gcc-11-base gcc-12
libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan8 libasan8
libatomic1 libblas3 libc-dev-bin libc-devtools libc6-dev libcairo2 libcc1-0 libcrypt-dev
libdatrie1 libdbi1 libdeflate0 libdpkg-perl libfakeroot libfile-fcntllock-perl libfontconfig1
libgcc-11-dev libgcc-12-dev libgd3 libgomp1 libgraphite2-3 libharfbuzz0b libhiredis0.14 libis123
libitm1 libjbig0 libjemalloc2 libjpeg-turbo8 libjpeg8 liblinear4 liblsan0 liblua5.1-0
liblua5.3-0 liblzf1 libmariadb3 libmpc3 libmysqlclient21 libnetfilter-queue1 libnorm1 libnsl-dev
libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpgm-5.3-0 libpixman-1-0 libquadmath0
libradcli4 librdkafka1 librrd8 libsensors-config libsensors5 libsnmp-base libsnmp40
libstdc++-11-dev libthai-data libthai0 libtiff5 libtirpc-dev libtsan0 libtsan2 libubsan1
libwebp7 libxcb-render0 libxcb-shm0 libxpm4 libxrender1 libzmq5 linux-libc-dev lto-disabled-list
lua-bitop lua-cjson lua-lpeg make manpages-dev mariadb-common mysql-common n2disk ndpi net-tools
nmap nmap-common nprobe ntop ntopng ntopng-data pfring pfring-dkms redis-server
redis-tools rpcsvc-proto
0 upgraded, 112 newly installed, 0 to remove and 3 not upgraded.
Need to get 185 MB of archives.
After this operation, 652 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



以下の画面のように、clickhouse-serverとntopngが再起動され、プロンプトが戻れば完了です

。



```
ntopng v6.0 script version - VMware Workstation 16 Player (非営利目的の使用のみ)
Player(P) | [Pause] [Mute] [Fullscreen] [Refresh] [Close]
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart networkd-dispatcher.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
+ sudo apt-get update
Hit:1 http://jp.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 https://packages.clickhouse.com/deb stable InRelease
Hit:3 http://jp.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://jp.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:5 http://jp.archive.ubuntu.com/ubuntu jammy-security InRelease
Get:6 https://packages.ntop.org/apt-stable/22.04 x64/ InRelease [2,153 B]
Get:7 https://packages.ntop.org/apt-stable/22.04 all/ InRelease [2,153 B]
Fetched 4,306 B in 7s (628 B/s)
Reading package lists... Done
+ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
 python3-update-manager ubuntu-advantage-tools update-manager-core
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
+ sudo sh -c 'echo '\'-F=clickhouse;127.0.0.1;ntopng;default;default\'' >> /etc/ntopng/ntopng.conf
+ sudo systemctl restart clickhouse-server
+ sudo systemctl restart ntopng
ntop@ntopngv6:/home$ _
```

コマンドでntopngの起動確認を行います。

```
$sudo systemctl status ntopng
● ntopng.service - ntopng high-speed web-based traffic monitoring and analysis>
  Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset>
  Active: active (running) since Thu 2024-01-04 10:22:57 JST; 1 min 44s ago
  Main PID: 2045 (ntopng-main)
  Tasks: 30 (limit: 4515)
  Memory: 219.0M
  CPU: 9.108s
  CGroup: /system.slice/ntopng.service
          mq2045/usr/bin/ntopng /run/ntopng.conf
```

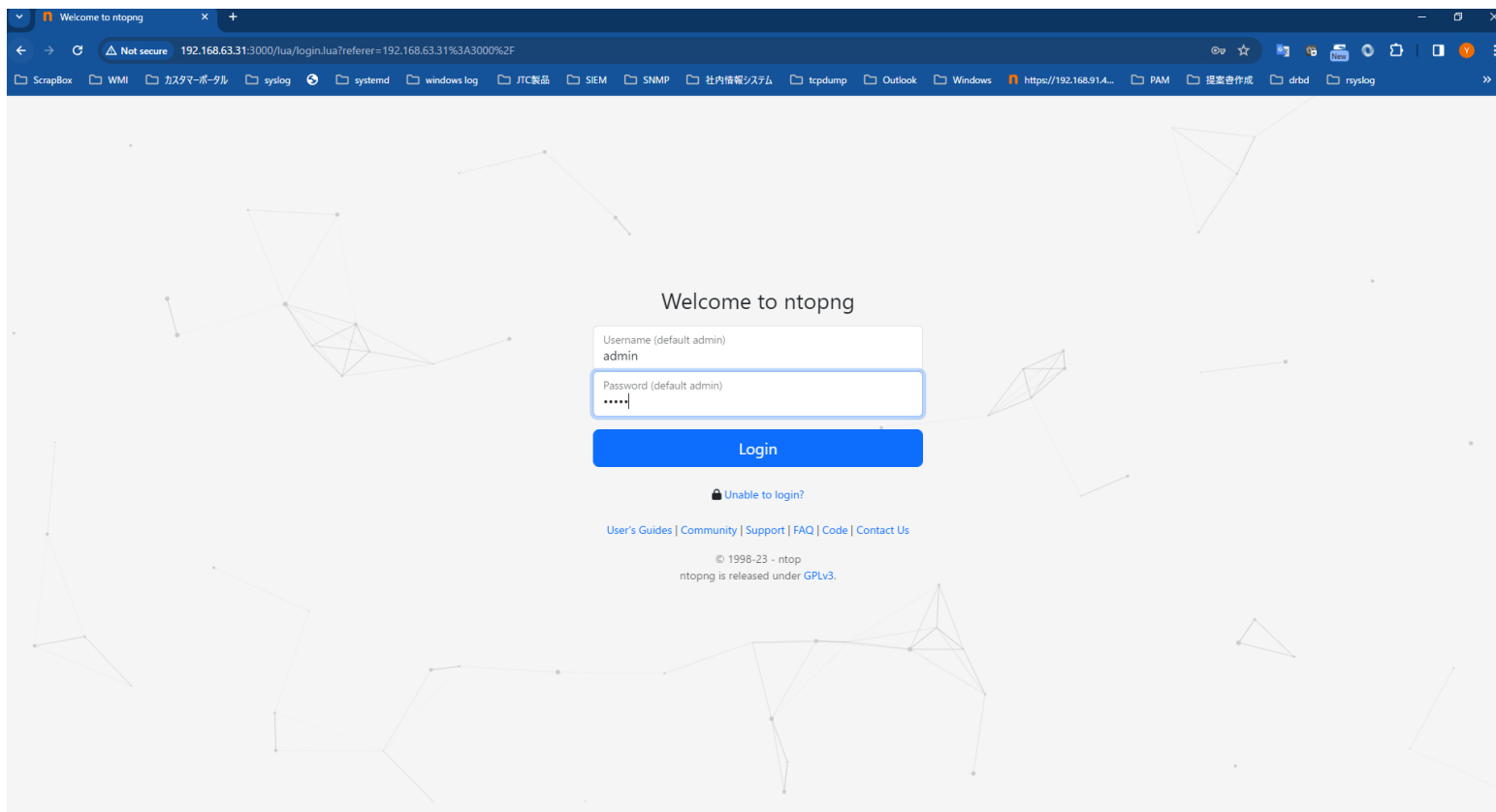
上記の標準出力のように、Active: activeとなっていればntopngは正常に起動しております。

コマンドで nProbeの起動確認を行います。

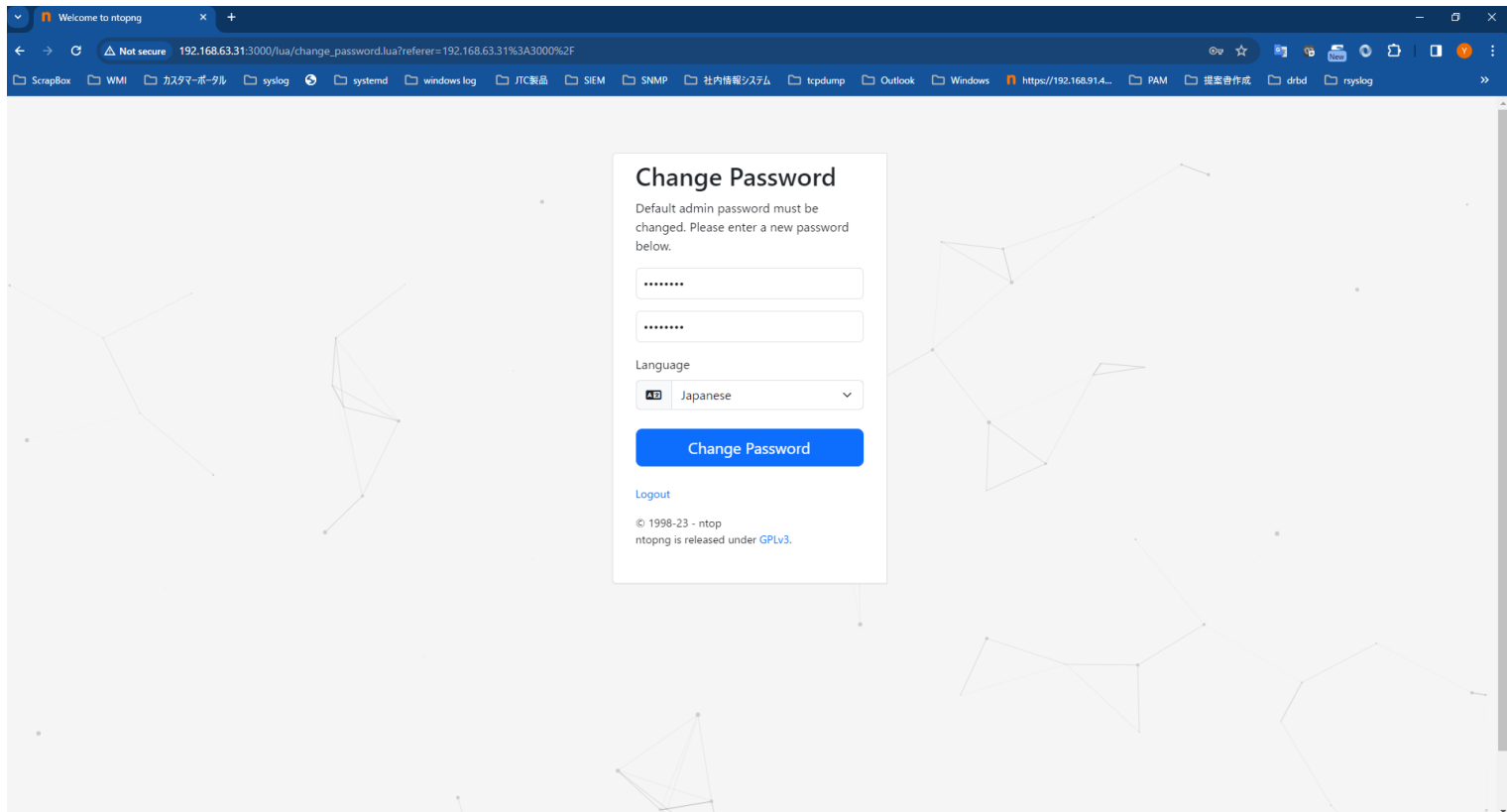
```
$sudo systemctl status nprobe
● nprobe.service - nprobe extensible NetFlow v5/v9/IPFIX probe/collector
   Loaded: loaded (/etc/systemd/system/nprobe.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-01-04 10:22:46 JST; 4min 44s ago
     Main PID: 1090 (nprobe@lo)
        Tasks: 4 (limit: 4515)
       Memory: 31.8M
          CPU: 6.156s
      CGroup: /system.slice/nprobe.service
             mq1090/usr/bin/nprobe /run/nprobe.conf
```

上記の標準出力のように、Active: activeとなっていればnprobeは正常に起動しております。

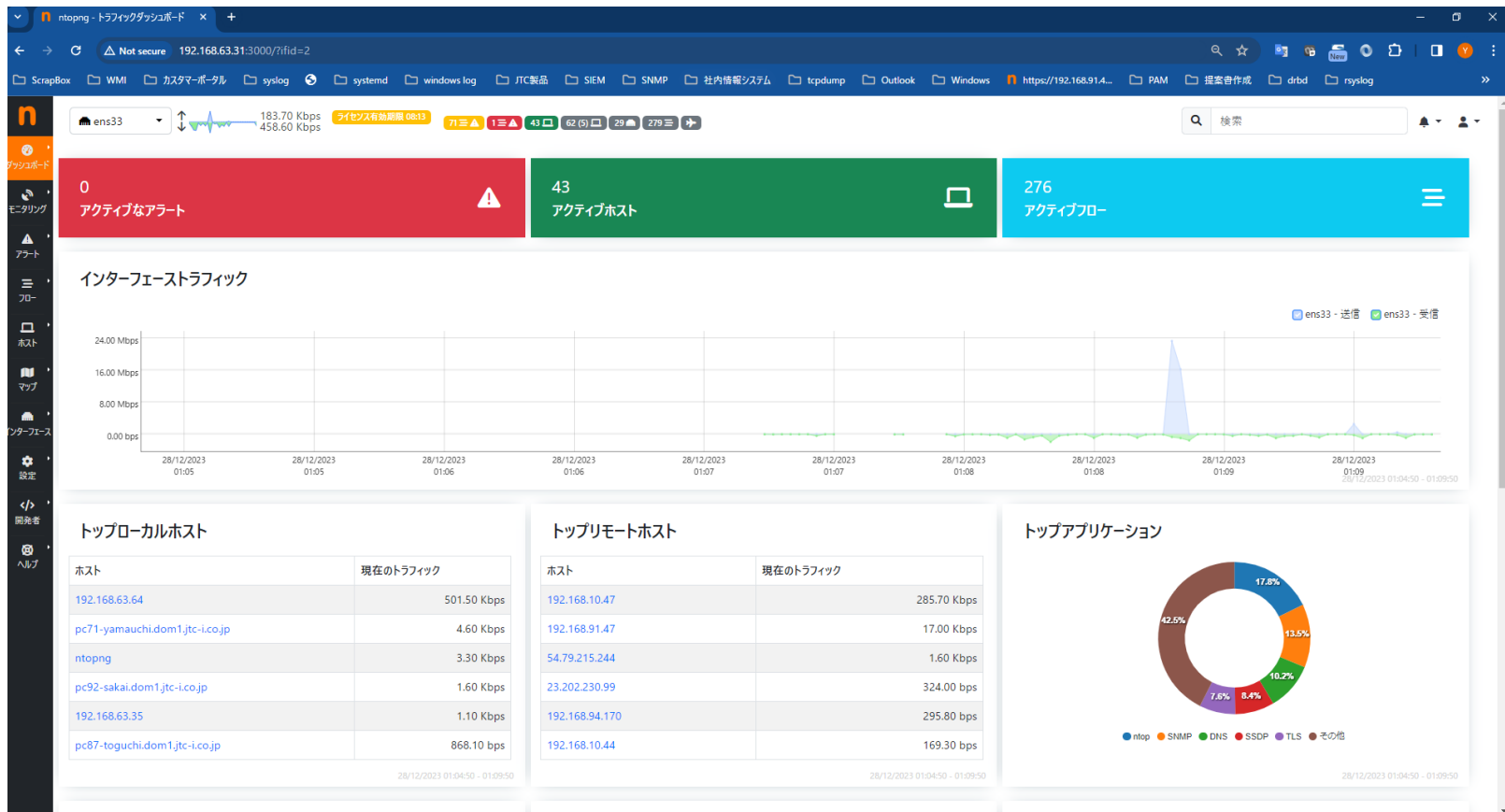
最後にWebブラウザでntopngの起動確認を行います。本ドキュメント” ISOインストール(14)”で設定したIPアドレス情報を使って、Webブラウザでアクセスします。<http://設定したIPアドレス:3000> を入力すると以下のWelcome画面が表示されます。admin/adminと入力し、「Login」ボタンをクリックします。



“Change Passowrd”画面が表示され、パスワード変更が求められますので任意のパスワードを設定してください。「Change Password」ボタンをクリックし、次に進んでください。



以下の画面の様にntopngのダッシュボードが表示されれば、起動確認は完了です。本画面のようなリッチな画面は商用版で起動している証拠です。10分経過するとフリー版の画面に遷移しますので適宜再起動をして商用版の機能をお楽しみください。



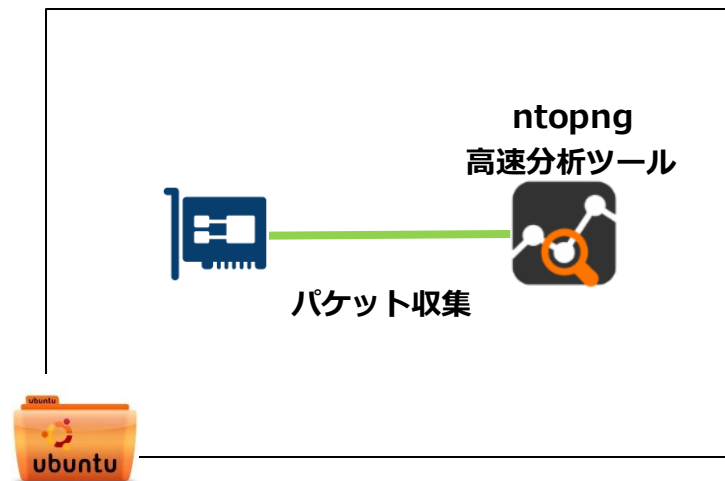
5. NIC直接監視評価パターン

本章では以下のバージョンを使用しています。

- ◆ Windows 11 x64
 - ◆ nProbe 10.X and ntopng v6.X Stable版
 - ◆ VMware Workstation 17
-

弊社サイトからダウンロードしたISOイメージは、ntopngが直接自NICを監視する設定が施してあります。本章では、下図の直接自PCのNICを監視する設定環境をご紹介します。

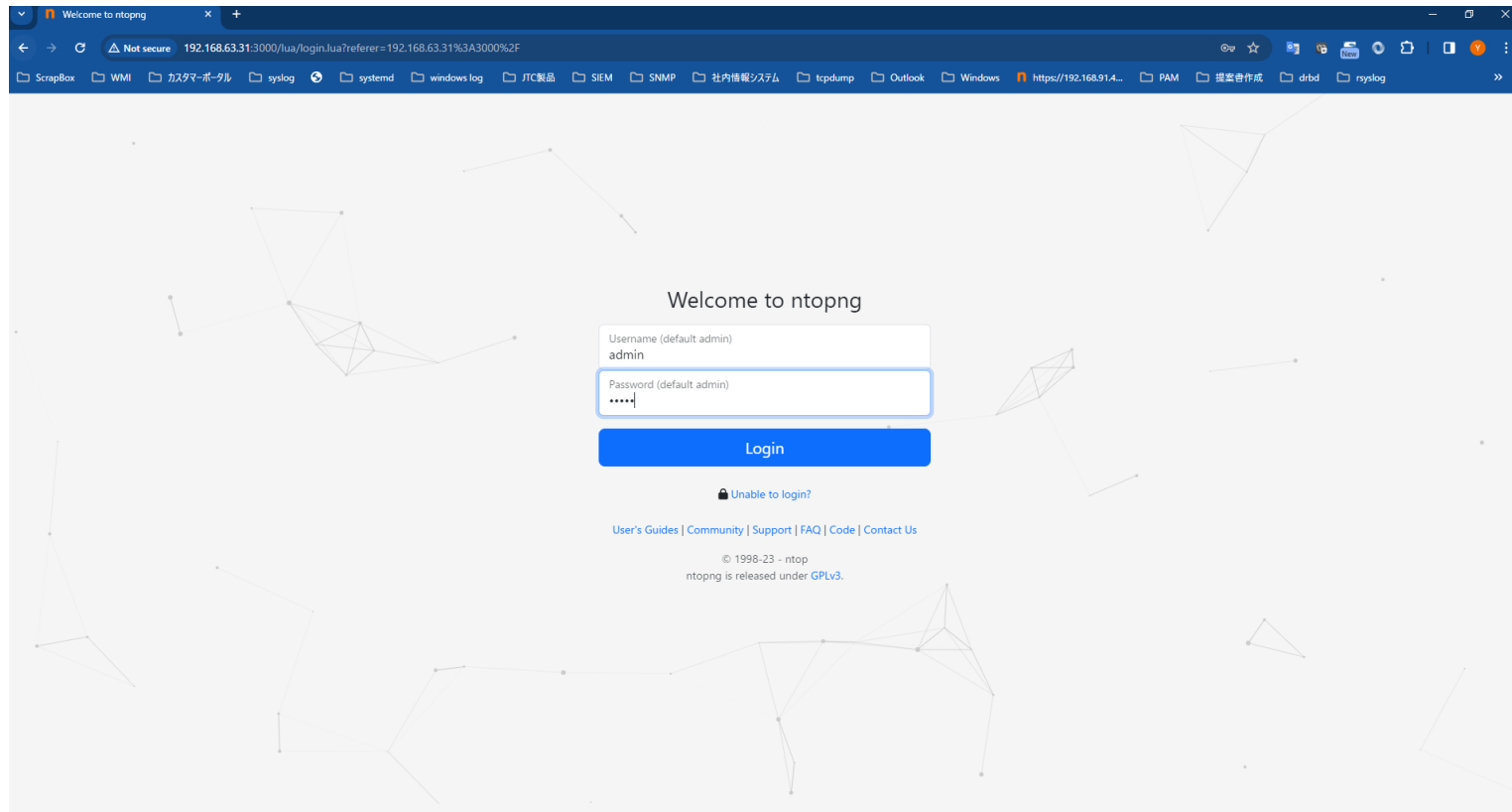
ntopngのNIC直接監視評価環境



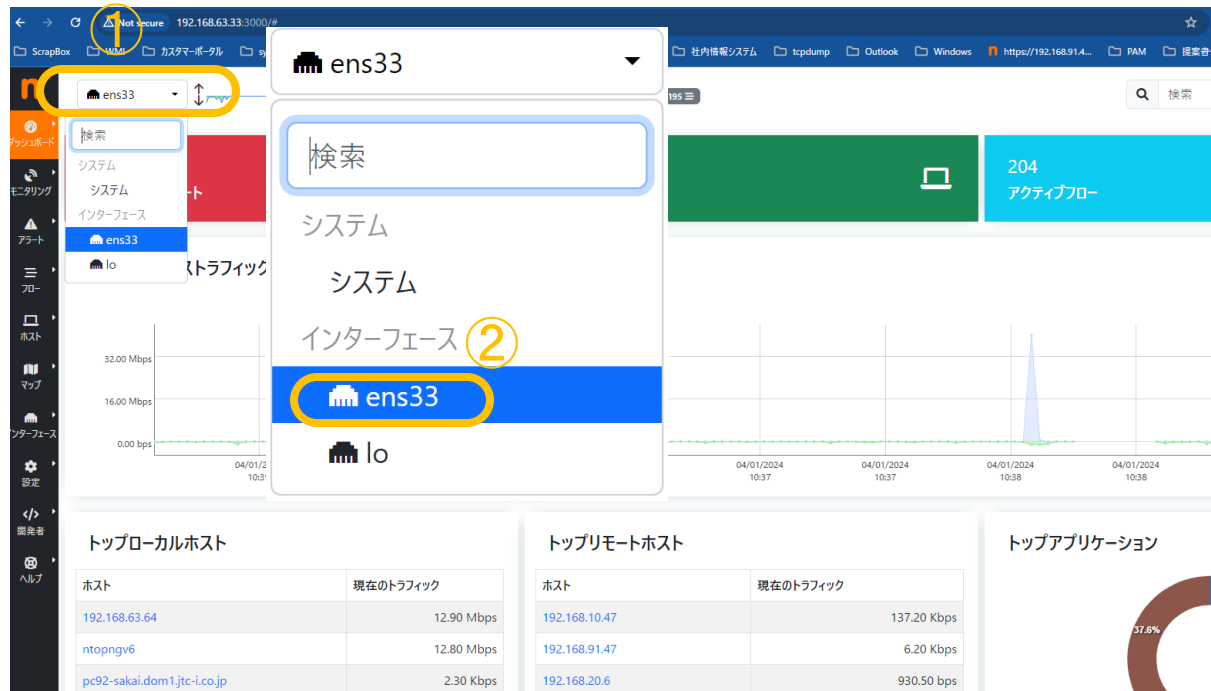


ntopngへのアクセス(1)

ntopngのWEBインターフェイスに進みます。http://<UbuntuのIPアドレス>:3000にアクセスしてください。ユーザ名:admin パスワード: ntopdemoでログインすると次スライドの画面が表示されます。

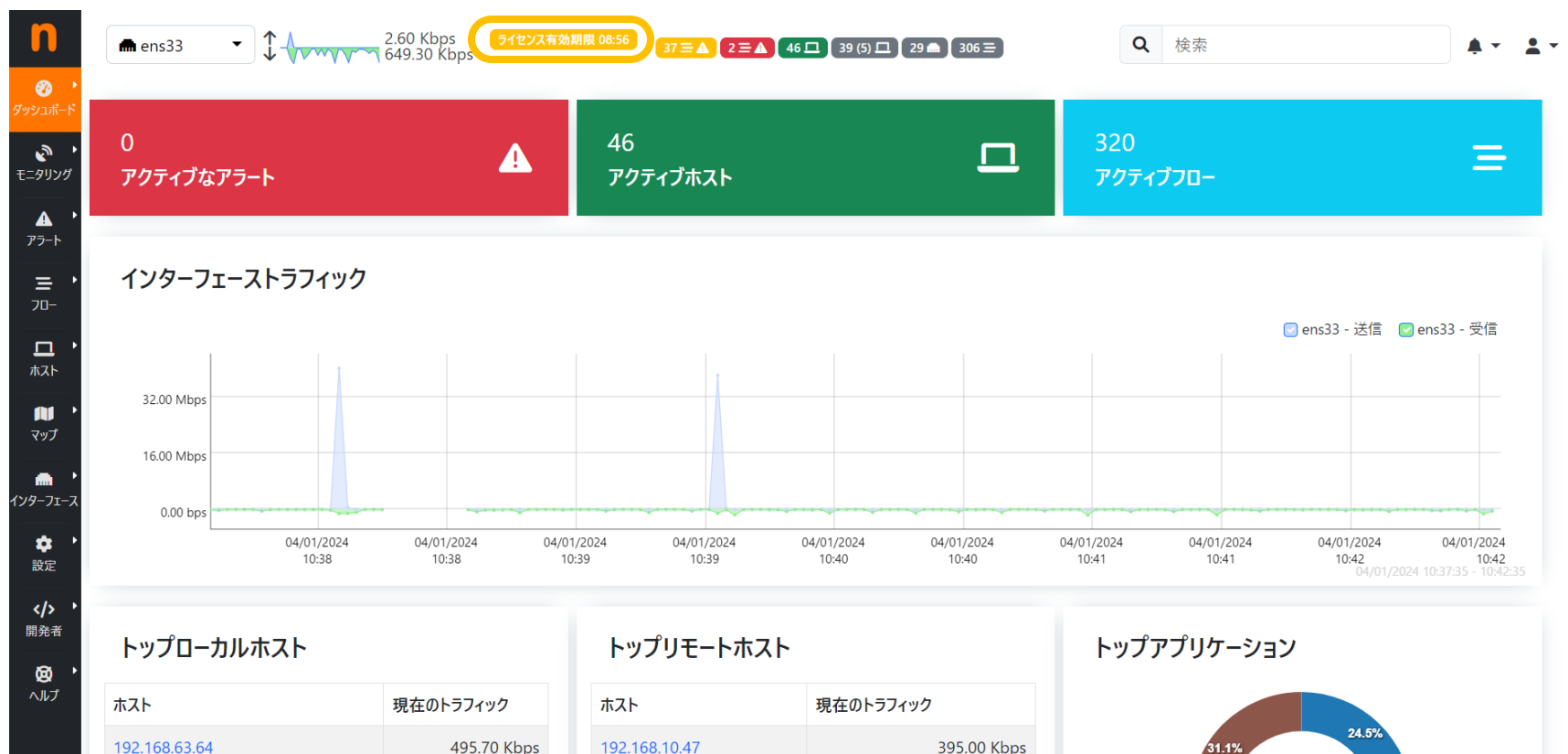


ntopngのWEBインターフェースに進みます。ログイン後画面左上のプルダウンメニューを押し、本マニュアル「初期設定(1)」で確認したデバイス名を選択してください。

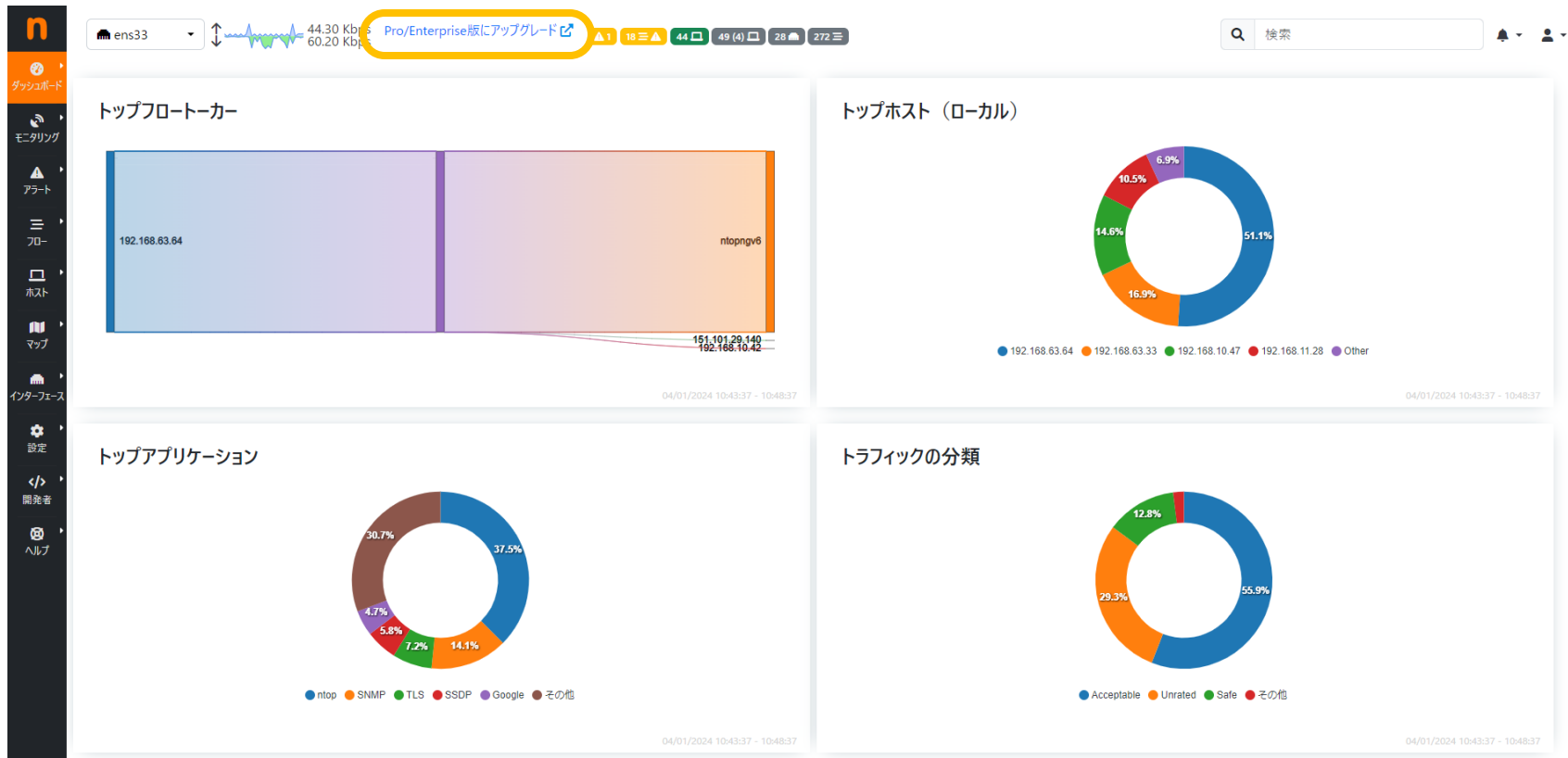


※本来であれば、ここで選択するデバイスは、ルータ、スイッチ等のミラーポートに接続されたデバイスとなります。本環境は、あくまでntopngの単体評価が目的なので自端末のネットワークに接続されたNICを監視対象としています。

選択したインターフェイスに流れるトラフィックが表示されます。最初に表示される画面は、トラフィックダッシュボードとなり、ローカルホスト及びリモートホストのトラフィックが表示されます。また、画面上部に「**ライセンスはXX:XXに期限切れします**」と表示されます。こちらの時間が0となると、ntopngはコミュニティ版にダウングレードします。



参考にコミュニティ版にダウングレードした場合のダッシュボード画面をご紹介します。有用な様々な画面が表示されなくなります。



6. ntopng Enterprise版評価方法

ntopngは起動から10分でコミュニティ版にダウングレードします。※10分間しかEnterprise版を評価できませんのでご注意ください。コミュニティ版とEnterprise版では大きく機能差があります。

Enterprise版評価を実行する為に、Webブラウザの右画面人型マークをクリックし、ntopngを再起動してください。



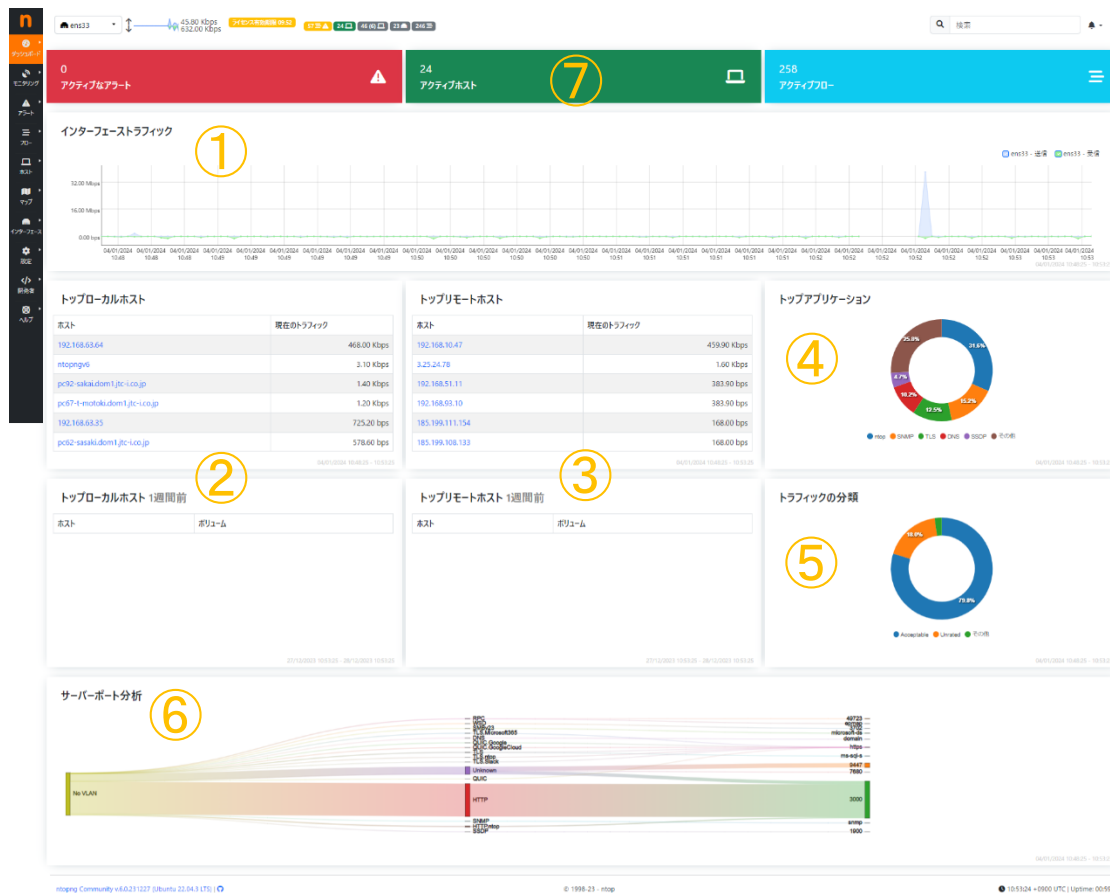
7. ntopng NIC直接監視評価 基本画面説明

ntopngは非常に多くの画面・グラフが存在します。本評価ガイドでは、その一部をご紹介します。

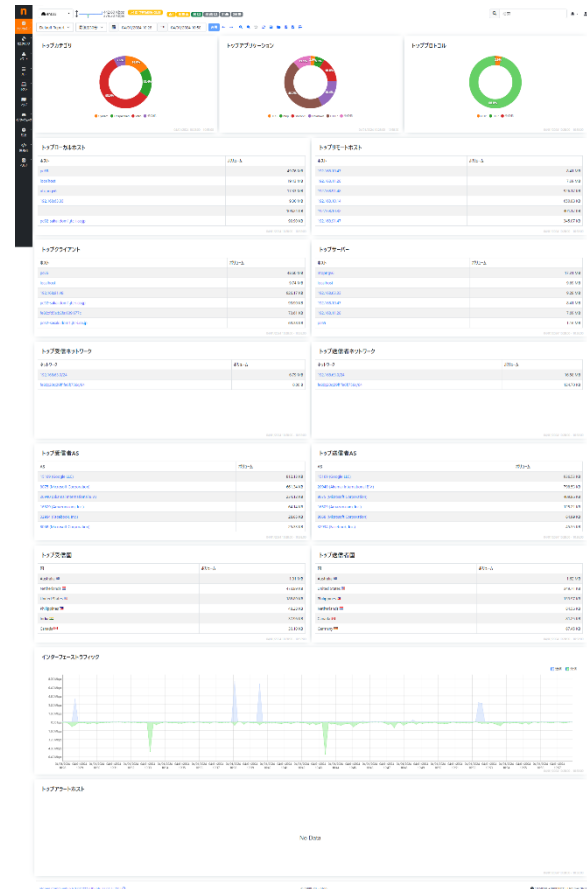
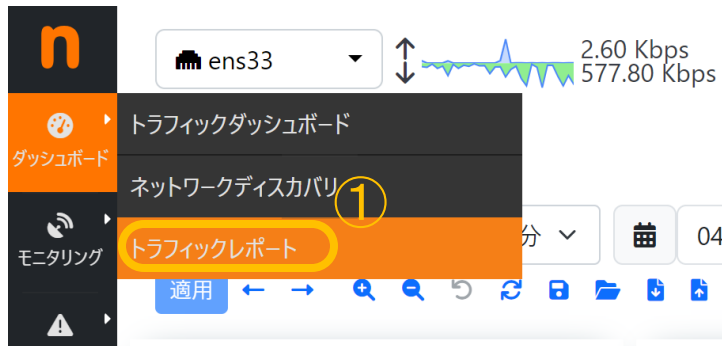
※より詳細に関しては、弊社デモをご用命ください。

トラフィックダッシュボード画面

ntopngのトップ画面「トラフィックダッシュボード」は、全てリアルタイム表示となり、次の7種類のトラフィック情報を確認できます。①「インターフェイストラフィック」②「トップローカルホスト」③「トップリモートホスト」④「トップアプリケーション」⑤「トラフィックの分類」⑥「サーバーポート分析」⑦「アクティブアラート/ホスト/フローへのリンク」があり、インターフェイストラフィックでは監視対象全てのインターフェイスのトラフィック量をリアルタイムで監視することができます。



画面左メニューの「ダッシュボード」から①「トラフィックレポート」をクリックすると、ネットワークインターフェイスのトラフィック量、ローカル/リモートの通信割合、アプリケーション、アプリケーショントラフィック割合、トップローカルホスト、トップリモートホストといった情報を日時を指定してレポートを作成することができます。本機能によって、日・週・月ごとのレポートを作成することができます。



画面左メニューの①「エクスプローラ」をクリックし、現在・過去に発生したアラートの一覧を確認することができます。本機能によって、監視ネットワークの異常をいち早く検知し、素早いアクションを起こすことが可能です。

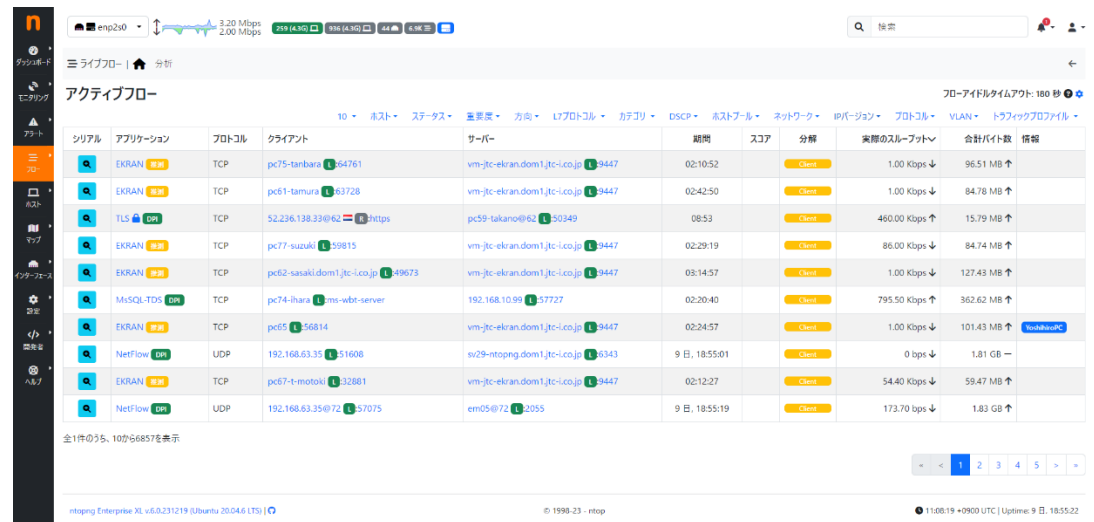


	注意またはそれ以下	警告	エラー	重大
インターフェース	0	0	14	0
ホスト	0	0	1,645	0
フロー	44,192	3	84,014	0
ユーザー	129	1	0	0
システム	1,446	0	3	0

ノート

- アラートは、現在アクティブ（トリガーされており、まだリリースされていない）場合、アクティブです。手動で分析し、アクションメニューを使用して確認する必要があるアラートは注意が必要です。すべてのアラート、注意が必要なものとシステムによって手動または自動で確認されるものは、すべてボックスに表示されます。

画面左メニューの「フロー」をクリックし「ライブ」を選択すると、リアルタイムで流れているフローの一覧が表示されます。アプリケーション、クライアント、サーバーといった項目はリンクとなっておりそれぞれのメニューにジャンプすることができます。また、フィルタに「ホスト」「状態」「方向」「アプリケーション」「カテゴリ」「IPバージョン」があり、それぞれソートすることができます。本機能によって、現在発生している通信をリアルタイムで確認することができます。

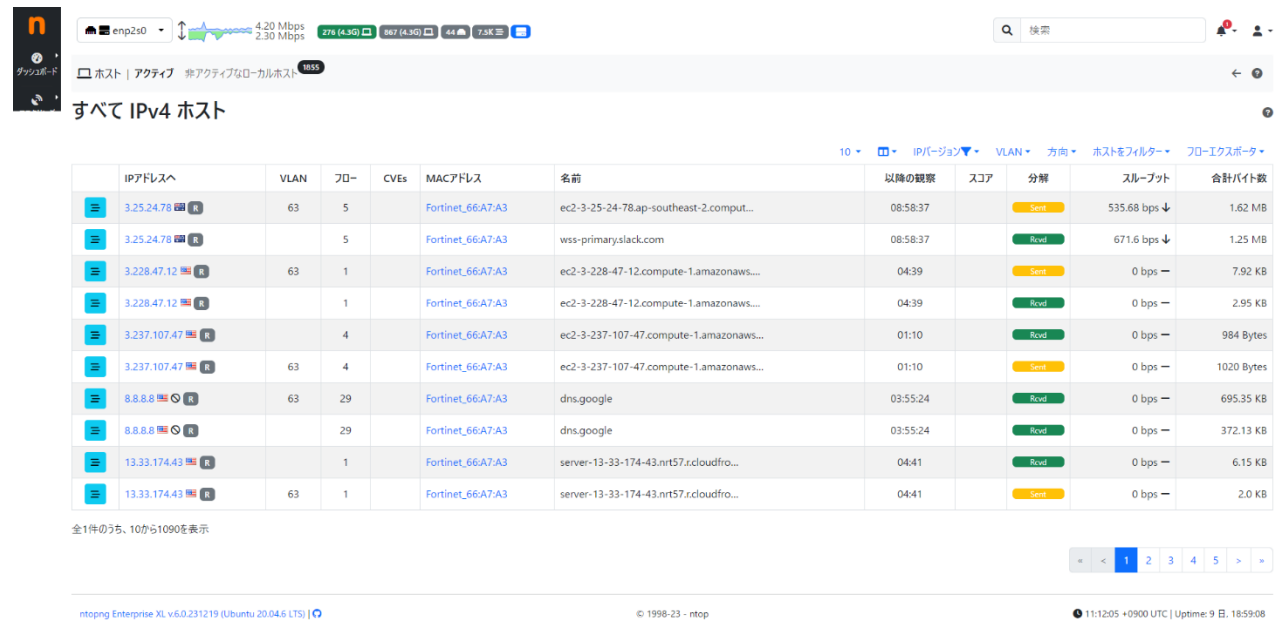



シリアル	アプリケーション	プロトコル	クライアント	サーバー	期間	スロア	分解	実際のスルーアウト	合計バイト数	情報
1	EKRAN	TCP	pc75-tanbara	vm-jtc-ekran.dom1.jtc-ico.jp	02:10:52	Client	Client	1.00 Kbps ↓	96.51 MB ↑	
2	EKRAN	TCP	pc61-tamura	vm-jtc-ekran.dom1.jtc-ico.jp	02:42:50	Client	Client	1.00 Kbps ↓	84.78 MB ↑	
3	TLS	TCP	52.236.138.33@62	pc59-takano@62	08:53	Client	Client	460.00 Kbps ↑	15.79 MB ↑	
4	EKRAN	TCP	pc77-suzuki	vm-jtc-ekran.dom1.jtc-ico.jp	02:29:19	Client	Client	86.00 Kbps ↓	84.74 MB ↑	
5	EKRAN	TCP	pc62-sasaki.dom1.jtc-ico.jp	vm-jtc-ekran.dom1.jtc-ico.jp	03:14:57	Client	Client	1.00 Kbps ↓	127.43 MB ↑	
6	MySQL-TDS	TCP	pc74-ihara	ms-wbt-server	02:20:40	Client	Client	795.50 Kbps ↑	362.62 MB ↑	
7	EKRAN	TCP	pc65	vm-jtc-ekran.dom1.jtc-ico.jp	02:24:57	Client	Client	1.00 Kbps ↓	101.43 MB ↑	Hostbaudc
8	NetFlow	UDP	192.168.63.31	sv29-ntopng.dom1.jtc-ico.jp	9日, 18:55:01	Client	Client	0 bps ↓	1.81 GB ↑	
9	EKRAN	TCP	pc67-i-motoki	vm-jtc-ekran.dom1.jtc-ico.jp	02:12:27	Client	Client	54.40 Kbps ↓	59.47 MB ↑	
10	NetFlow	UDP	192.168.63.35@72	em05@72	9日, 18:55:19	Client	Client	173.70 bps ↓	1.83 GB ↑	

全1件の35、10の66857を表示

ntop Enterprise XL v6.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop | 11:08:19 +0900 UTC | Update: 9日, 18:55:22

画面左メニューの「ホスト」から「ホスト」をクリックすると、アクティブなホスト一覧が表示されます。IPアドレスはリンクになっています。「分解」はトラフィック送受の割合。ホストごとの「スループット」、「合計バイト」を確認できます。さらに詳細はIPアドレスのリンクをクリックするとそれぞれのホストごとのトラフィックを解析することができます。

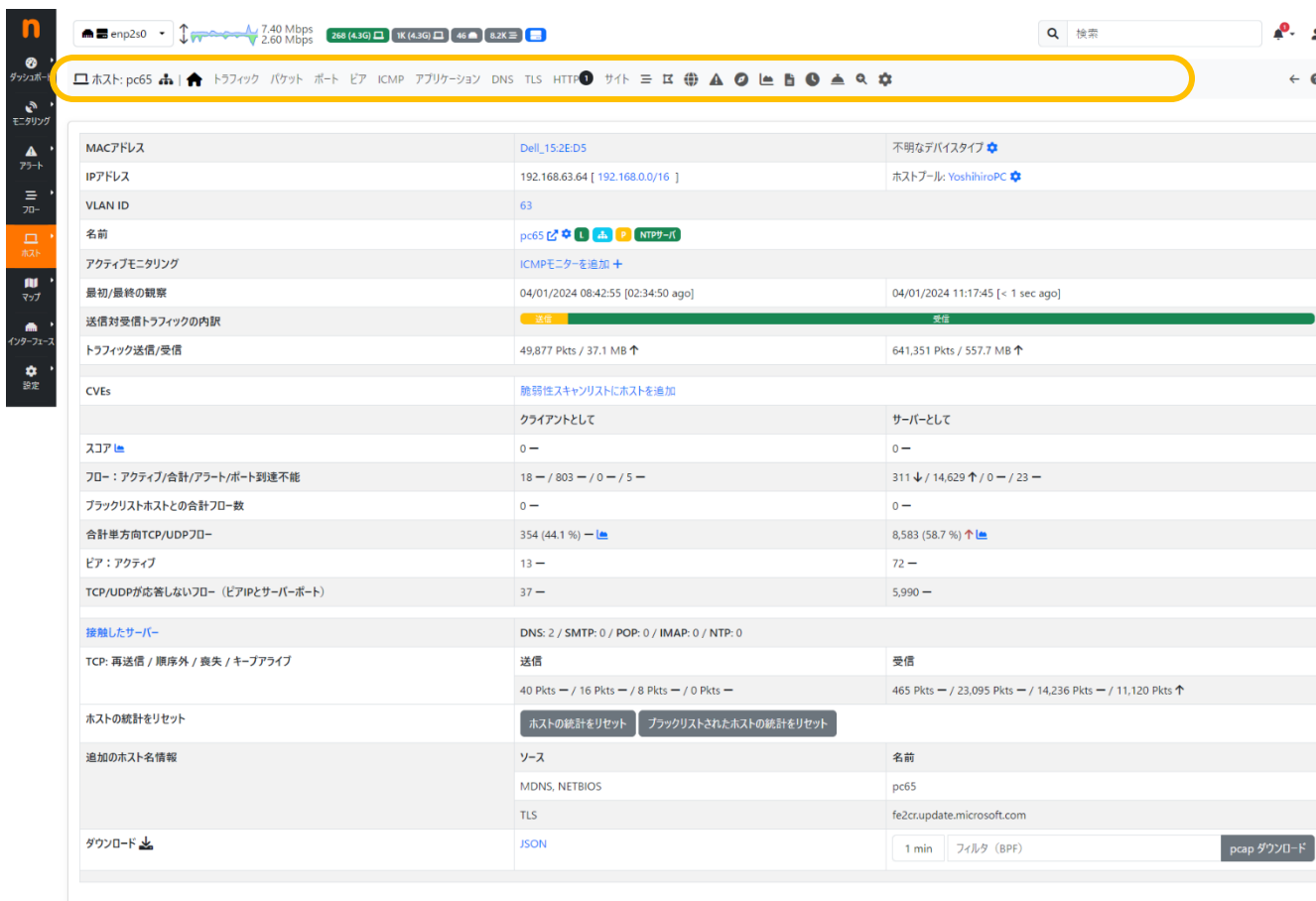
すべて IPv4 ホスト

IPアドレス	VLAN	フロー	CVEs	MACアドレス	名前	以降の観察	スコア	分解	スループット	合計バイト数
3.25.24.78	63	5		Fortinet_66:A7:A3	ec2-3-25-24-78.ap-southeast-2.comput...	08:58:37		Sent	535.68 bps ↓	1.62 MB
3.25.24.78		5		Fortinet_66:A7:A3	wss-primary.slack.com	08:58:37		Recv	671.6 bps ↓	1.25 MB
3.228.47.12	63	1		Fortinet_66:A7:A3	ec2-3-228-47-12.compute-1.amazonaws...	04:39		Sent	0 bps —	7.92 KB
3.228.47.12		1		Fortinet_66:A7:A3	ec2-3-228-47-12.compute-1.amazonaws...	04:39		Recv	0 bps —	2.95 KB
3.237.107.47		4		Fortinet_66:A7:A3	ec2-3-237-107-47.compute-1.amazonaws...	01:10		Recv	0 bps —	984 Bytes
3.237.107.47	63	4		Fortinet_66:A7:A3	ec2-3-237-107-47.compute-1.amazonaws...	01:10		Sent	0 bps —	1020 Bytes
8.8.8.8	63	29		Fortinet_66:A7:A3	dns.google	03:55:24		Recv	0 bps —	695.35 KB
8.8.8.8		29		Fortinet_66:A7:A3	dns.google	03:55:24		Recv	0 bps —	372.13 KB
13.33.174.43		1		Fortinet_66:A7:A3	server-13-33-174-43.nrt57.r.cloudfro...	04:41		Recv	0 bps —	6.15 KB
13.33.174.43	63	1		Fortinet_66:A7:A3	server-13-33-174-43.nrt57.r.cloudfro...	04:41		Sent	0 bps —	2.0 KB

全1件のうち、10から1090を表示

ntopng Enterprise XL v6.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop | 11:12:05 +0900 UTC | Uptime: 9 日, 18:59:08

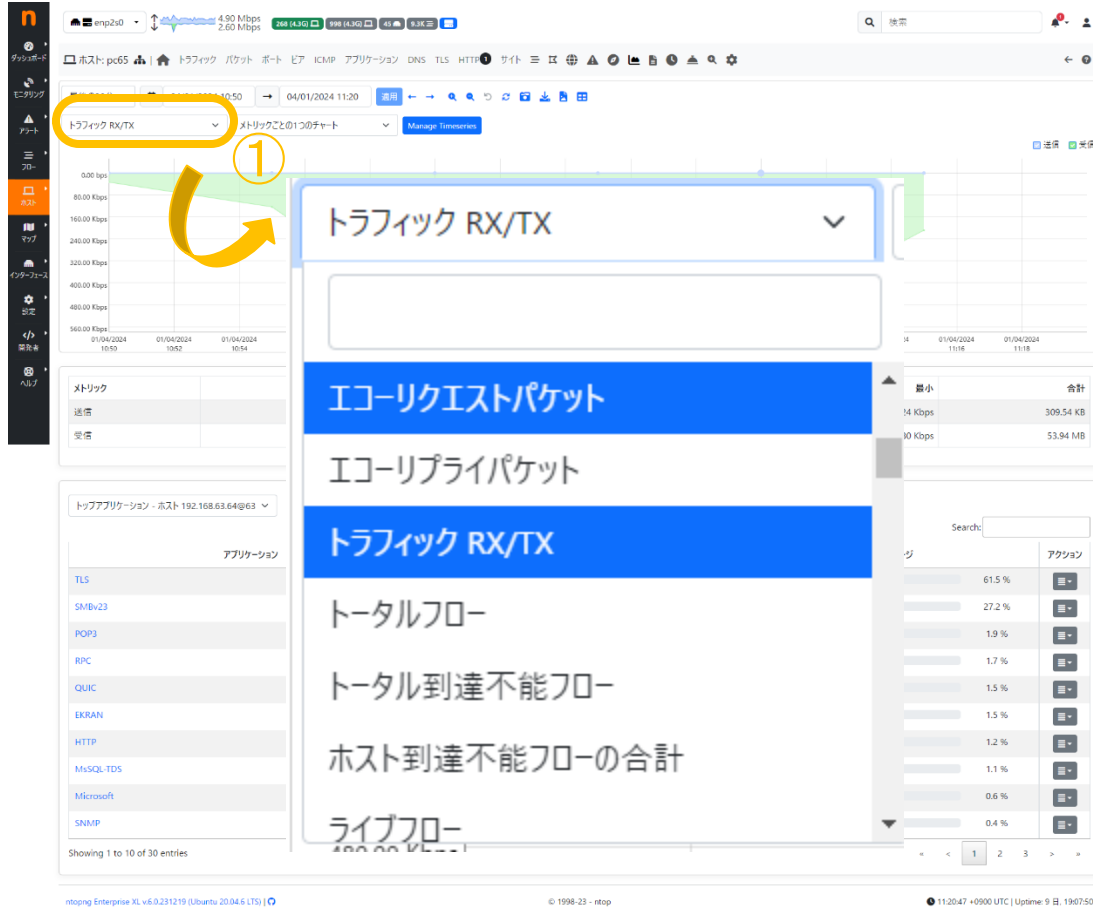
画面は「pc65」をクリックしたものです。メニューに「ホーム」「トラフィック」「パケット」「ポート」「ピア」「ICMP」「アプリケーション」..「グラフ」「設定」等のメニューがあり、ホスト単位に分析をすることができます。



The screenshot shows the ntopng interface for host 'pc65'. The browser address bar is highlighted in yellow, showing the URL: `http://192.168.0.16/hosts/pc65`. The main content area displays a table of host information and statistics.

MACアドレス	Dell_15_2E_D5	不明なデバイスタイプ
IPアドレス	192.168.63.64 [192.168.0.0/16]	ホストフル: YoshihiroPC
VLAN ID	63	
名前	pc65	NTPサーバー
アクティブモニタリング	ICMPモニターを追加 +	
最初/最終の観測	04/01/2024 08:42:55 [02:34:50 ago]	04/01/2024 11:17:45 [< 1 sec ago]
送信対受信トラフィックの内訳	送信 受信	
トラフィック送信/受信	49,877 Pkts / 37.1 MB ↑	641,351 Pkts / 557.7 MB ↑
CVEs	脆弱性スキャンリストにホストを追加	
スコア	クライアントとして	サーバーとして
フロー: アクティブ/合計/アラート/ポート到達不能	18 - / 803 - / 0 - / 5 -	311 ↓ / 14,629 ↑ / 0 - / 23 -
ブラックリストホストとの合計フロー数	0 -	0 -
合計単方向TCP/UDPフロー	354 (44.1 %) ↓	8,583 (58.7 %) ↑
ピア: アクティブ	13 -	72 -
TCP/UDPが応答しないフロー (ピアIPとサーバーポート)	37 -	5,990 -
接触したサーバー	DNS: 2 / SMTP: 0 / POP: 0 / IMAP: 0 / NTP: 0	
TCP: 再送信 / 順序外 / 喪失 / キープアライブ	送信	受信
	40 Pkts - / 16 Pkts - / 8 Pkts - / 0 Pkts -	465 Pkts - / 23,095 Pkts - / 14,236 Pkts - / 11,120 Pkts ↑
ホストの統計をリセット	ホストの統計をリセット ブラックリストされたホストの統計をリセット	
追加のホスト名情報	ソース	名前
	MDNS, NETBIOS	pc65
	TLS	fe2c2r.update.microsoft.com
ダウンロード	JSON	1 min フィルタ (BPF) pcap ダウンロード

画面は「pc65」の「グラフアイコン」クリックした画面です。該当ホストのみのトラフィック情報が表示され、過去～現在のトラフィックを分析することができます。画面①のプルダウンをクリックするとL4/L7/カテゴリといったより詳細な項目で該当ホストのトラフィック分析ができます。



The screenshot shows the ntop interface for host 'pc65'. The main chart area displays 'トラフィック RX/TX' (Traffic RX/TX) with a Y-axis ranging from 0.00 Kbps to 560.00 Kbps and an X-axis showing time from 01/04/2024 10:50 to 10:54. A dropdown menu is open, showing the following options:

- トラフィック RX/TX
- Eコーリクエストパケット
- Eコーリプライパケット
- トラフィック RX/TX
- トータルフロー
- トータル到達不能フロー
- ホスト到達不能フローの合計
- ライブフロー

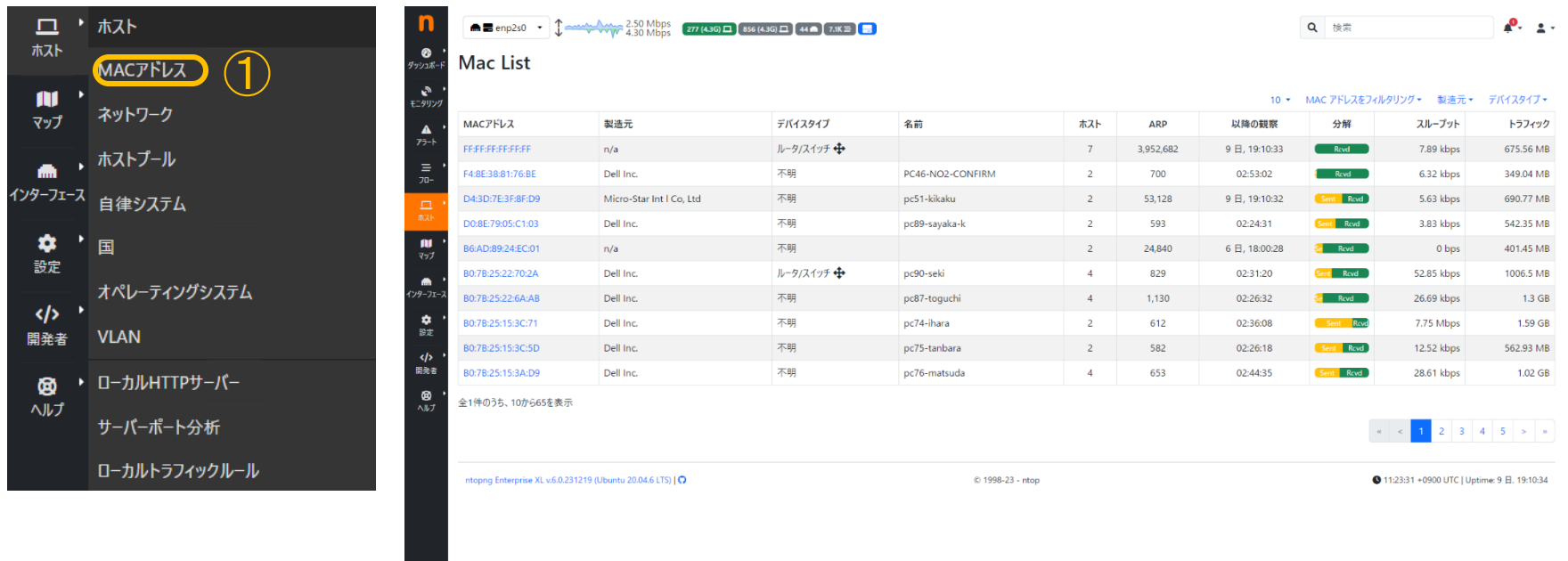
On the right side, there is a table showing traffic statistics:

器小	合計
14 Kbps	309.54 KB
10 Kbps	53.94 MB

At the bottom, there is a table showing application traffic:

アプリ	割合	アクション
61.5 %	[-]	
27.2 %	[-]	
1.9 %	[-]	
1.7 %	[-]	
1.5 %	[-]	
1.5 %	[-]	
1.2 %	[-]	
1.1 %	[-]	
0.6 %	[-]	
0.4 %	[-]	

画面左メニューの「ホスト」から「MACアドレス」をクリックすると、所属ネットワーク内で確認できるMACアドレス一覧を表示し、ホストのトラフィック情報を表示します。さらに詳細はMACアドレスのリンクをクリックすれば、ホストごとのトラフィックを解析することができます。



Mac List

MACアドレス	製造元	デバイスタイプ	名前	ホスト	ARP	以降の観察	分解	スループット	トラフィック
FF:FF:FF:FF:FF:FF	n/a	ルータ/スイッチ		7	3,952,682	9日, 19:10:33	Rcvd	7.89 kbps	675.56 MB
F4:8E:38:81:76:BE	Dell Inc.	不明	PC46-NO2-CONFIRM	2	700	02:53:02	Rcvd	6.32 kbps	349.04 MB
D4:3D:7E:3F:8F:D9	Micro-Star Int l Co, Ltd	不明	pc51-kikaku	2	53,128	9日, 19:10:32	Sent Rcvd	5.63 kbps	690.77 MB
D0:8E:79:05:C1:03	Dell Inc.	不明	pc89-sayaka-k	2	593	02:24:31	Sent Rcvd	3.83 kbps	542.35 MB
B6:AD:89:24:EC:01	n/a	不明		2	24,840	6日, 18:00:28	Sent Rcvd	0 bps	401.45 MB
B0:7B:25:22:70:2A	Dell Inc.	ルータ/スイッチ	pc90-seki	4	829	02:31:20	Sent Rcvd	52.85 kbps	1006.5 MB
B0:7B:25:22:6A:AB	Dell Inc.	不明	pc87-toguchi	4	1,130	02:26:32	Sent Rcvd	26.69 kbps	1.3 GB
B0:7B:25:15:3C:71	Dell Inc.	不明	pc74-ihara	2	612	02:36:08	Sent Rcvd	7.75 Mbps	1.59 GB
B0:7B:25:15:3C:5D	Dell Inc.	不明	pc75-tanbara	2	582	02:26:18	Sent Rcvd	12.52 kbps	562.93 MB
B0:7B:25:15:3A:D9	Dell Inc.	不明	pc76-matsuda	4	653	02:44:35	Sent Rcvd	28.61 kbps	1.02 GB

全1件のうち、10から65を表示

ntopng Enterprise XL v.6.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop 11:23:31 +0900 UTC | Uptime: 9日, 19:10:34

画面左メニューの「ホスト」から「ネットワーク」をクリックすると、所属ネットワークで確認できるサブネットごとのトラフィック状況を確認することができます。②のサブネットリンクと③グラフリンクをクリックすると、トラフィック詳細を解析することができます。



The screenshot shows the ntop network management interface. On the left is a sidebar menu with 'ネットワーク' (Network) highlighted and circled with a '1'. The main area displays a table of networks with columns for network name, host count, score, ratio, and traffic. Two columns, 'ネットワーク名' (Network Name) and 'チャート' (Chart), are circled with a '2' and '3' respectively. Below the table is a note about duplicate networks.

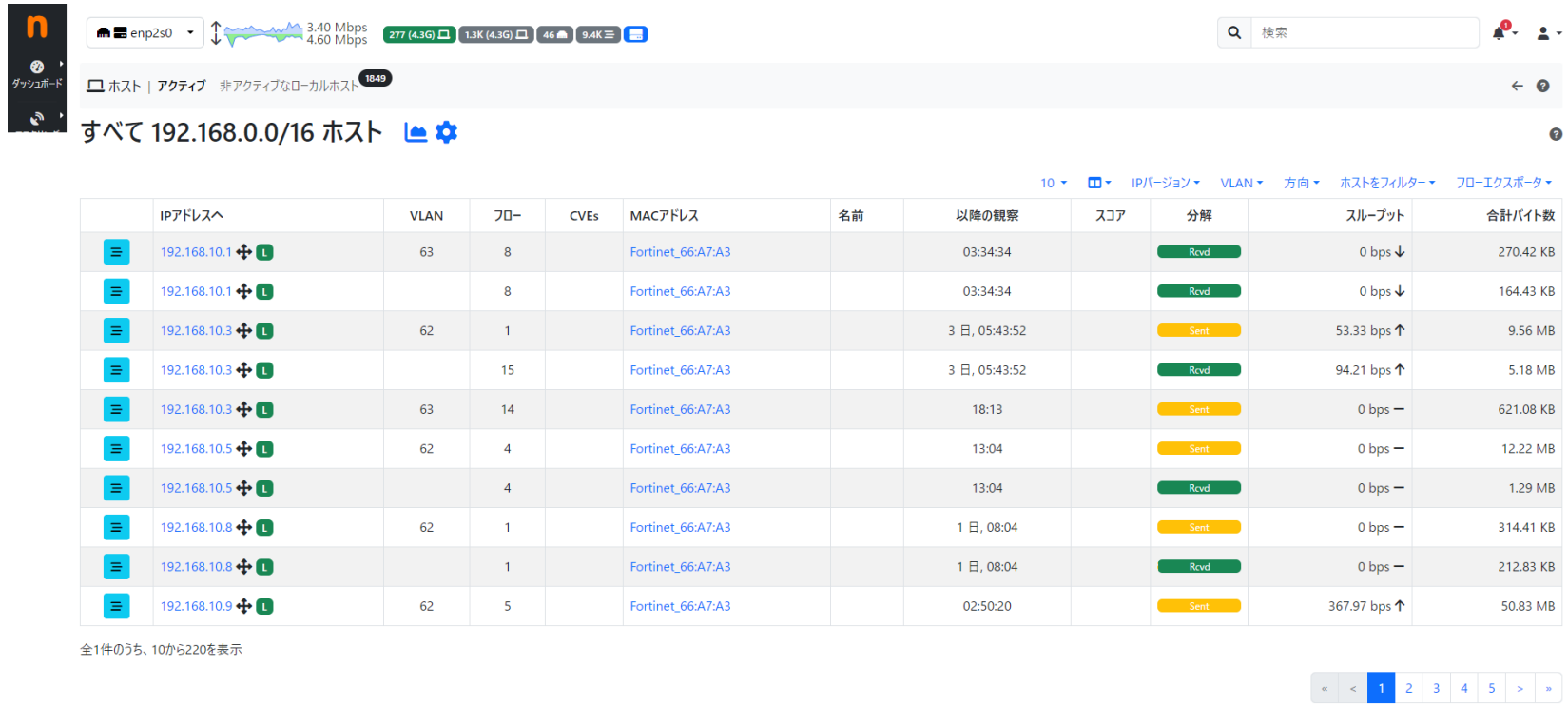
ネットワーク名	チャート	ホスト	スコア	ホスト/スコア比	アラートされたフロー	分解	スループット	トラフィック
fe80:82ee:73ff:fe1:bd8/64		28				Sent	11.51 kbps	148.81 MB
192.168.0.0/16		225				Sent Rcvd	5.09 Mbps	228.26 GB
172.16.0.0/12						Rcvd	0 bps	1.91 KB
10.0.0.0/8						Rcvd	0 bps	238.54 KB

全1件のうち、4から4を表示

ノート
重複するネットワークが定義されている場合：
1. 上記の表には両方のネットワークエントリが表示されます。
2. 広範なネットワークには、より小さなネットワークで定義されたホストは含まれません。

ntopng Enterprise XL v6.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop | 11:28:33 +0900 UTC | Uptime: 9 日, 19:15:36

画面は、前スライドページ(ネットワーク画面(1))の「192.168.0.0/16」サブネットリンクをクリックしたものです。サブネットに所属しているホストの一覧が表示されます。



Dashboard: enp2s0 | 3.40 Mbps / 4.60 Mbps | 277 (4.3G) | 1.3K (4.3G) | 46 | 9.4K

検索

ホスト | アクティブ | 非アクティブなローカルホスト | 1849

すべて 192.168.0.0/16 ホスト

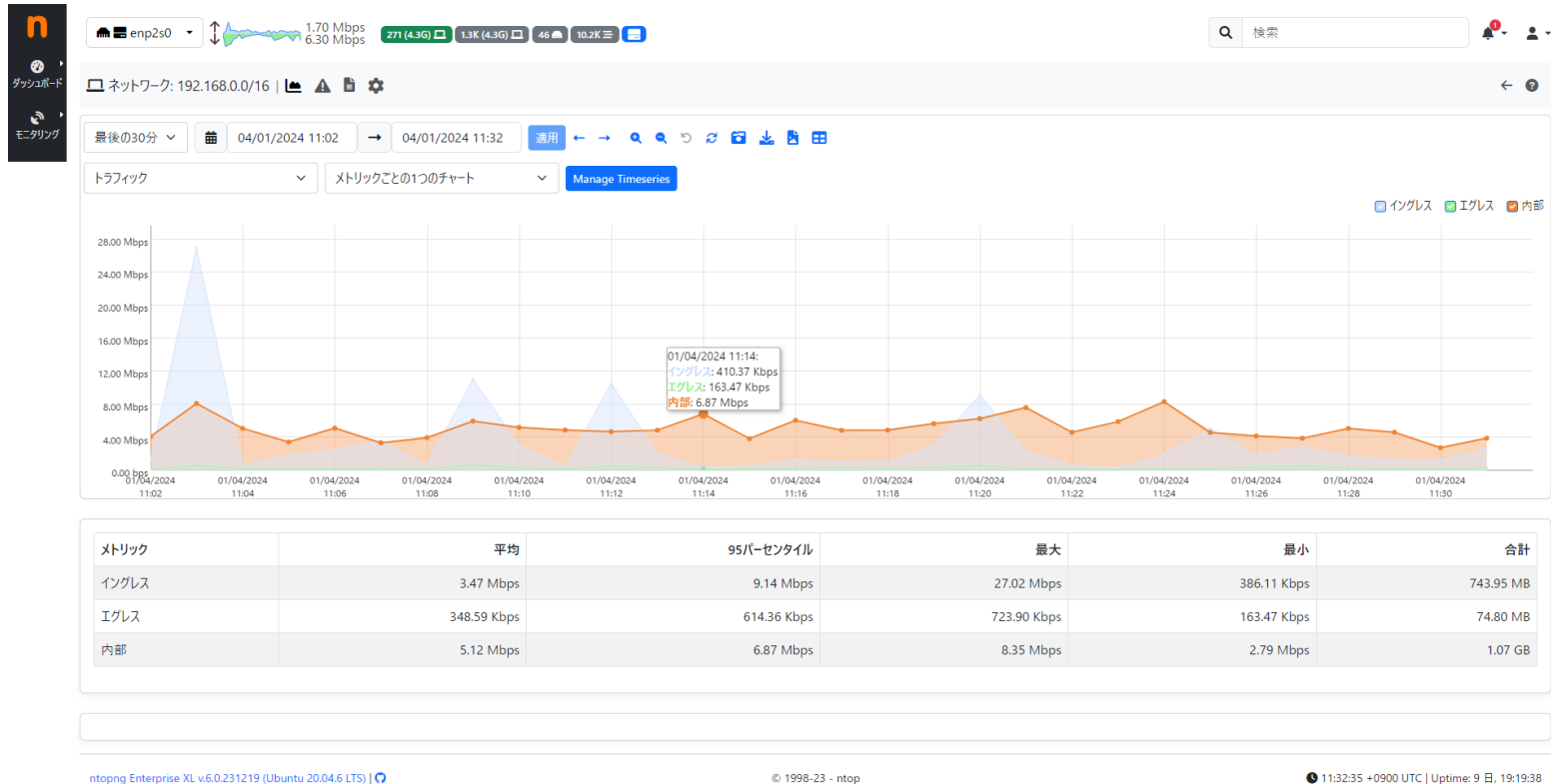
10 | IPバージョン | VLAN | 方向 | ホストをフィルター | フローエクスポート

	IPアドレス	VLAN	フロー	CVEs	MACアドレス	名前	以降の観察	スコア	分解	スループット	合計バイト数
☰	192.168.10.1	63	8		Fortinet_66:A7:A3		03:34:34		Rcvd	0 bps ↓	270.42 KB
☰	192.168.10.1		8		Fortinet_66:A7:A3		03:34:34		Rcvd	0 bps ↓	164.43 KB
☰	192.168.10.3	62	1		Fortinet_66:A7:A3		3 日, 05:43:52		Sent	53.33 bps ↑	9.56 MB
☰	192.168.10.3		15		Fortinet_66:A7:A3		3 日, 05:43:52		Rcvd	94.21 bps ↑	5.18 MB
☰	192.168.10.3	63	14		Fortinet_66:A7:A3		18:13		Sent	0 bps —	621.08 KB
☰	192.168.10.5	62	4		Fortinet_66:A7:A3		13:04		Sent	0 bps —	12.22 MB
☰	192.168.10.5		4		Fortinet_66:A7:A3		13:04		Rcvd	0 bps —	1.29 MB
☰	192.168.10.8	62	1		Fortinet_66:A7:A3		1 日, 08:04		Sent	0 bps —	314.41 KB
☰	192.168.10.8		1		Fortinet_66:A7:A3		1 日, 08:04		Rcvd	0 bps —	212.83 KB
☰	192.168.10.9	62	5		Fortinet_66:A7:A3		02:50:20		Sent	367.97 bps ↑	50.83 MB

全1件のうち、10から220を表示

« < 1 2 3 4 5 > »

画面は、前スライドページ(ネットワーク画面(1))の「192.168.0.0/24」グラフィックをクリックしたものです。中長期視点で対象とする時間帯を絞った分析をすることができます。



画面左メニュー「ホスト」から「ホストプール」をクリックすると、ホストプールリスト画面が表示されます。②の「歯車」ボタンを押すとホストプールの編集をすることができます。設定した「プール名」リンクをクリックすると、ホストプールの詳細トラフィック情報を確認することができます。



The screenshot shows the ntop interface with the 'Host Pools' menu item highlighted in the left sidebar (marked with a circled '1'). The main content area displays a table of host pools. A gear icon (marked with a circled '2') is located next to the 'Host Pools List' header. Below the table, there is a footer with version information and a timestamp.

プール名	チャート	ホスト	以降の観察	分解	スループット	トラフィック
iperfTest		1	9 日, 19:22:10		0 bps	1.16 GB
YoshihiroPC		1	9 日, 19:22:10		63.47 kbps	8.75 GB
Jupiter Engineer		27	01:00		138.81 kbps	1.78 MB
Jailed Hosts			9 日, 19:22:10		0 bps	0 Bytes
Default		1,466	9 日, 19:22:10		7.13 Mbps	228.72 GB

全1件のうち、5から5を表示

ntopng Enterprise XL v.6.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop 11:35:06 +0900 UTC | Uptime: 9 日, 19:22:09

画面は別途作成した「Jupiter Engineer」ホストプール画面となります。設定したサブネット通りの表示になっていることが確認できます。本機能を利用して組織・部署といったサブネット区分けができる環境であればサブネットごとのトラフィック量や分析が容易となります。

	IPアドレス	VLAN	ポート	CVEs	MACアドレス	名前	以降の観察	スコア	分解	スループット	合計バイト数
	192.168.63.1	63	13		Fortinet_66:A7:A3		6 日, 16:31:15		Sent	0 bps ↓	97.98 MB
	192.168.63.33	63	1		VMware_6F:75:6C		00:55 sec		Rcvd	0 bps →	110 Bytes
	192.168.63.35	63	10		ICANNIAN_00:01:0A		9 日, 19:24:33		Rcvd	0 bps ↓	787.46 MB
	192.168.63.43	63	294		Dell_22:6A:AB	pc87-toguchi	02:40:33		Rcvd	7.15 kbps ↓	560.34 MB
	192.168.63.44	63	41		Dell_05:C1:03	pc89-sayaka-k	02:38:32		Rcvd	4.2 kbps ↑	157.35 MB
	192.168.63.45	63	234		Dell_4B:EF:2E	pc92-sakai	02:51:32		Rcvd	81.01 kbps ↑	294.16 MB
	192.168.63.48	63	294		Dell_15:35:A5	pc66-yasuda	02:44:03		Rcvd	179.36 kbps ↑	656.26 MB
	192.168.63.49	63	68		Dell_15:2D:49	pc61-tamura	03:12:30		Rcvd	186.64 bps ↓	1017.87 MB
	192.168.63.50	63	313		Dell_15:35:C7	pc62-sasaki	03:44:09		Rcvd	56.37 kbps ↑	663.57 MB
	192.168.63.51	63	41		Dell_15:35:B2	pc71-yamauchi.dom1.jtc-i.co.jp	9 日, 19:24:33		Rcvd	691.91 bps ↓	2.0 GB

全1件のうち、10から26を表示

画面左メニューの「インターフェイス」から「詳細」、そして「アプリケーション」を選択した画面です。この画面でL7トラフィックまで確認することができ、対象インターフェイスの利用状況・どのアプリケーションが帯域を占有しているかを確認することができます。

The screenshot displays the ntop web interface for interface `enp2s0`. The left sidebar shows the navigation menu with 'インターフェイス' (Interface) selected. The main content area is divided into several sections:

- インターフェイス詳細 (Interface Details):** Shows basic information for `enp2s0`, including its status (アップライブ), name, MTU (1518 bytes), and family (PF_RING RX/TX).
- トラフィックの分解 (Traffic Breakdown):** A donut chart showing traffic distribution by destination, with Remote-Local at 41.8%.
- トラフィック統計 (Traffic Statistics):** A table of traffic metrics:

トラフィックの異常	ローカルホストの異常
合計トラフィック	238.1 GB [397,056,866 Pkts]
送信トラフィック	74.5 GB [148,917,993 Pkts]
- アプリケーション概要 (Application Summary):** A large donut chart showing the top applications consuming bandwidth.

アプリケーション	割合
ADS_Analytic_Track	41.8%
ARP	27.4%
AWAST	14.0%
AdultContent	15.8%
- アプリケーション詳細 (Application Details):** A table listing specific applications and their bandwidth usage:

アプリケーション	合計 (総動員)	パーセンテージ
ADS_Analytic_Track	143.11 MB	0.1%
ARP	273.16 MB	0.1%
AWAST	96.33 KB	0.0%
AdultContent	41.28 MB	0.0%

Annotations in the image include a red circle around the '詳細' (Details) menu item and a red circle around the 'アプリケーション' (Application) menu item in the top navigation bar. A red arrow points from the application summary chart to the application details table.

8. ntopng+nProbe xFlow受信評価パターン

本章では以下の設定方法をご案内します。

1. ntopng and nProbe評価環境
 2. ntopng設定変更
 3. nProbe設定変更
 4. ntopng正常動作確認
-

ntopng+nprobe環境を評価するには以下の準備が必要です。まずはnprobeの設定変更を実施します。

```
$cd /etc/nprobe
$sudo cp -p nprobe.conf.ntopng.sample nprobe.conf
$sudo vim nprobe.conf
~snip~
#--collector-port=6363
--collector-port=2055
~snip~
:wq!
$sudo systemctl restart nprobe
$ sudo systemctl status nprobe
● nprobe.service - nprobe extensible NetFlow v5/v9/IPFIX probe/collector
   Loaded: loaded (/etc/systemd/system/nprobe.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-01-04 11:49:06 JST; 4s ago
```

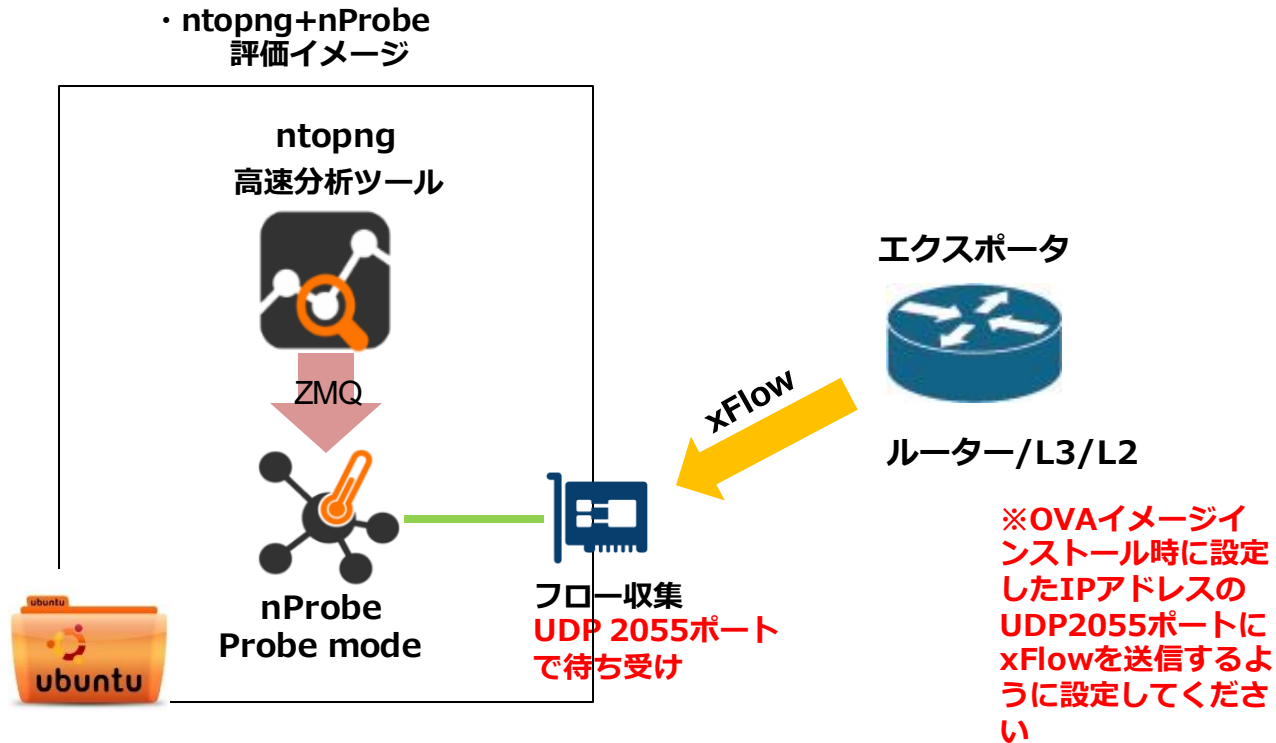
上記の標準出力のように、Active: activeとなっていればnprobeは正常に起動しております。上記では、nprobeの受信ポートを6363/udpから2055/udpに変更しております。

次にntopngの設定変更を実施します。以下では、ntopng.confに-i=で始まる2行を追加しております。-i=ens33の設定は、環境によって異なりますので適宜ご自身のNICデバイス名を確認し変更してください。

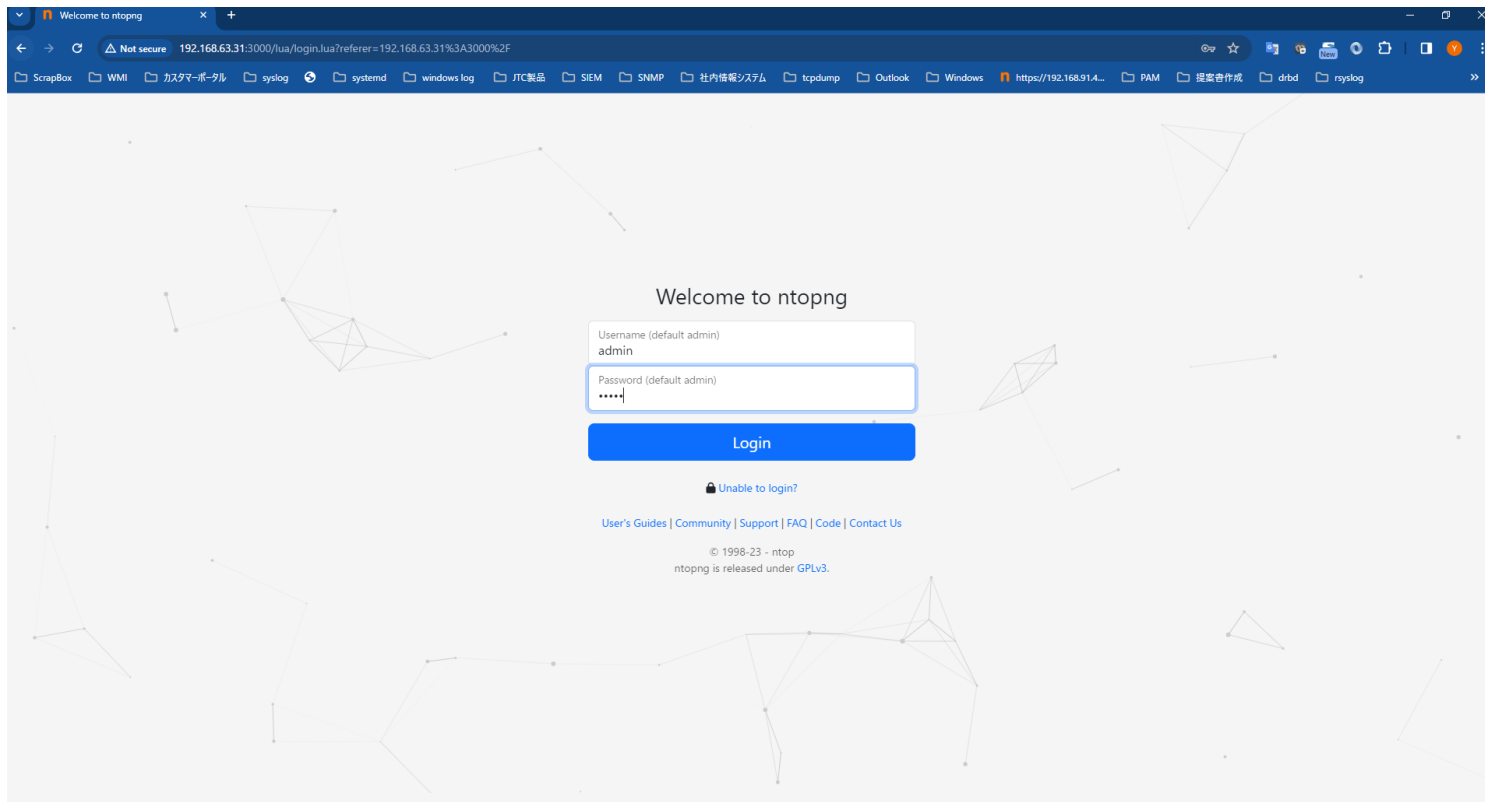
```
$cd /etc/ntopng
$sudo vim ntopng.conf
~snip~
-F=clickhouse;127.0.0.1;ntopng;default;default
-i=tcp://127.0.0.1:5556
-i=ens33
~snip~
:wq!
$ sudo systemctl status ntopng
● ntopng.service - ntopng high-speed web-based traffic monitoring and analysis tool
   Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-01-04 11:57:25 JST; 4s ago
```

上記の標準出力のように、Active: activeとなっていればntopngは正常に起動しております。

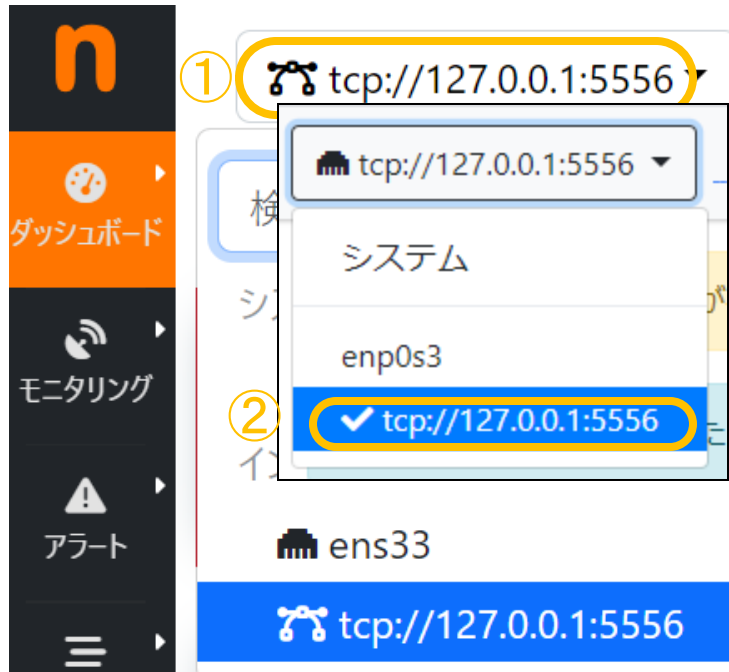
貴社設置のルーター等がxFlow(NetFlow v9/v5, sflow v5等)をエクスポートできる場合、本モードを利用してフローを収集することができます。



ntopngのWEBインターフェイスに進みます。http://<UbuntuのIPアドレス>:3000にアクセスしてください。ログインすると次スライドの画面が表示されます。

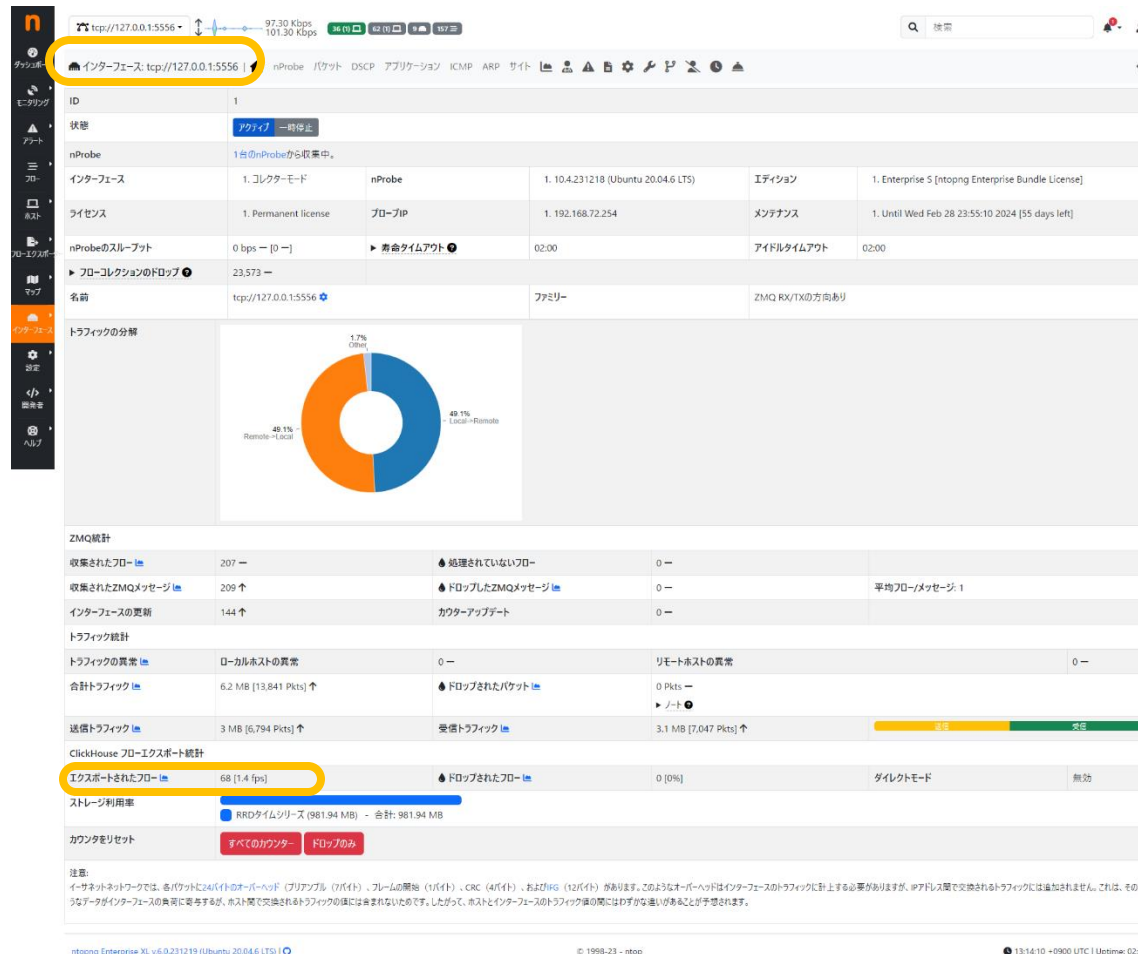


ntopngのWEBインターフェースに進みます。ログイン後画面左上のプルダウンメニューを押し、本マニュアル「tcp://127.0.0.1:5556」を選択してください。



※「enp0s3」がUbuntuのNICを監視するインターフェイス。「tcp://127.0.0.1:5556」がxFlowを受信するインターフェイスとなります。

①「tcp://127.0.0.1:5556」が選択されていることを確認し、画面左メニューの「インターフェイス」を押してください。xFlowを正しく受信している場合は画面中段に「エクスポートされたフロー」がカウントアップされます。



The screenshot shows the ntopng web interface for the interface 'tcp://127.0.0.1:5556'. The 'Exported Flows' section is highlighted with a yellow circle, showing 68 flows at 1.4 f/s. The 'Status' is 'Active' and 'nProbe' is '1 nProbe from collection'. The 'Traffic Breakdown' chart shows 49.1% Remote (Local) and 49.1% Local (Remote). The 'ZMQ Statistics' table shows 207 flows collected, 209 ZMQ messages, and 144 interface updates. The 'Traffic Statistics' table shows 6.2 MB of total traffic and 3 MB of outgoing traffic. The 'ClickHouse Export Statistics' table shows 68 exported flows at 1.4 f/s. The 'Storage Usage' section shows 981.94 MB of data. The 'Reset Counters' section has buttons for 'Reset All Counters' and 'Reset Drops Only'.

ID	1
状態	アクティブ 一時停止
nProbe	1台のnProbeから収集中。
インターフェイス	1. コレクターモード nProbe 1. 104.231219 (Ubuntu 20.04.6 LTS) エディション 1. Enterprise S (ntopng Enterprise Bundle License)
ライセンス	1. Permanent license プローブIP 1. 192.168.72.254 メンテナンス 1. Until Wed Feb 28 23:55:10 2024 [55 days left]
nProbeのスループット	0 bps [0 -] ▶ 寿命タイムアウト 02:00 アイドルタイムアウト 02:00
▶ フローコレクションのドロップ	23,573 -
名前	tcp://127.0.0.1:5556 ファミリー ZMQ RX/TXの方向あり

ZMQ統計			
収集されたフロー	207 ↓	処理されていないフロー	0 ↓
収集されたZMQメッセージ	209 ↑	ドロップしたZMQメッセージ	0 ↓
インターフェイスの更新	144 ↑	カウンターアップデート	0 ↓

トラフィック統計				
トラフィックの異常	ローカルホストの異常	0 ↓	リモートホストの異常	0 ↓
合計トラフィック	6.2 MB [13,841 Pkts] ↑	ドロップされたパケット	0 Pkts ↓	
送信トラフィック	3 MB [6,794 Pkts] ↑	受信トラフィック	3.1 MB [7,047 Pkts] ↑	

ClickHouse フローエクスポート統計			
エクスポートされたフロー	68 [1.4 f/s]	ドロップされたフロー	0 [0%]
ストレージ利用率	RRDタイムシリーズ (981.94 MB) - 合計: 981.94 MB		

カウンタをリセット すべてのカウンター ドロップのみ

注意:
インターフェイスのトラフィックは、各パケットに4バイトのオーバーヘッド (フラグメント (4バイト) + フレームの開始 (4バイト) + CRC (4バイト) + 64ビット) があります。このオーバーヘッドはインターフェイスのトラフィックに計上する必要はありません。@アドレス間で交換されるトラフィックには追加されません。これは、そのより大きなインターフェイスの負荷に発生するが、ホスト間で交換されるトラフィックの値には含まれないためです。したがって、ホストとインターフェイスのトラフィック値の間にはわずかな違いがあることが予想されます。

ntopng Enterprise XL v5.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop 13:14:10 +0900 UTC | Uptime: 0:229

画面左メニューの「フローエクスポート」、「フローエクスポートデバイス」を押してください。Ubuntuに設定したIPアドレスのUDP2055ポートにxFlowを送信しているエクスポートが存在する場合は、「フローエクスポートIP」にエクスポートのIPアドレスが表示されます。



The screenshot shows the ntopng web interface. The left sidebar has a menu with 'フローエクスポート' (Flow Export) and 'フローエクスポートデバイス' (Flow Exporter Devices) highlighted. The main content area is titled 'すべてのフローエクスポートデバイス' (All Flow Exporter Devices). It displays a table with the following data:

フローエクスポートIP	チャート	SNMPデバイス名	SNMPの説明	SNMP場所
192.168.11.1		一致するSNMPデバイスが見つかりません。		
192.168.63.35		一致するSNMPデバイスが見つかりません。		

The table shows two entries for flow exporter devices. The first entry has IP 192.168.11.1 and the second has IP 192.168.63.35. Both entries show '一致するSNMPデバイスが見つかりません。' (No matching SNMP device found). The interface also shows a search bar, a 'Show 10 entries' dropdown, and a 'Showing 1 to 2 of 2 entries' indicator. At the bottom, there is a footer with 'ntopng Enterprise XL v6.0.231219 (Ubuntu 20.04.6 LTS) | © 1998-23 - ntop | 13:17:23 +0900 UTC | Uptime: 05:42'.

※画面操作は、NICの直接監視と同様となります。また、エクスポートごとに仮想インターフェイスを作成することも可能です。詳細は弊社までお問い合わせください。

ジュピターテクノロジー株式会社

〒183-0023

東京都府中市宮町一丁目40番地

KDX府中ビル6F

Tel 042-358-1250

Fax 042-360-6221

URL <http://www.jtc-i.co.jp/>

技術サポートに関するお問合せ

<https://www.jtc-i.co.jp/support/customerportal/index.php>