JATP環境構築マニュアル 02.WEB COLLECTOR編

ジュニパーネットワークス株式会社

2018年8月28日

JUNIPER NETWORKS | Engineering Simplicity

はじめに

- 本資料にある内容は、資料作成時点におけるものであり、事前の予告なしに内容を変更する場合があります。
- 本資料は内容の正確さを保つために努めて作成しておりますが、本資料を利用することによって生じた損害について、当社は一切責任を負わないものとします。
- また、本資料の内容と公式情報との間に差分がある場合、公式情報を正としてお取り扱いください。
- 本資料は下記のソフトウェア/サービスを用いてJATPのセットアップを行っています。
  - JATP(OVA版/OVF版) v5.0.2
  - ESXi/vCenter Server 5.5

© 2019 Juniper Networks
Juniper Business Use Only

更新履歴

バージョン	更新日	更新内容
1.0	2018/08/28	初版公開
1.1	2018/12/17	vSwitchのVLANタグ設定を追記
1.2	2019/07/30	マニュアルのフォーマットを変更

© 2019 Juniper Networks

Juniper Business Use Only

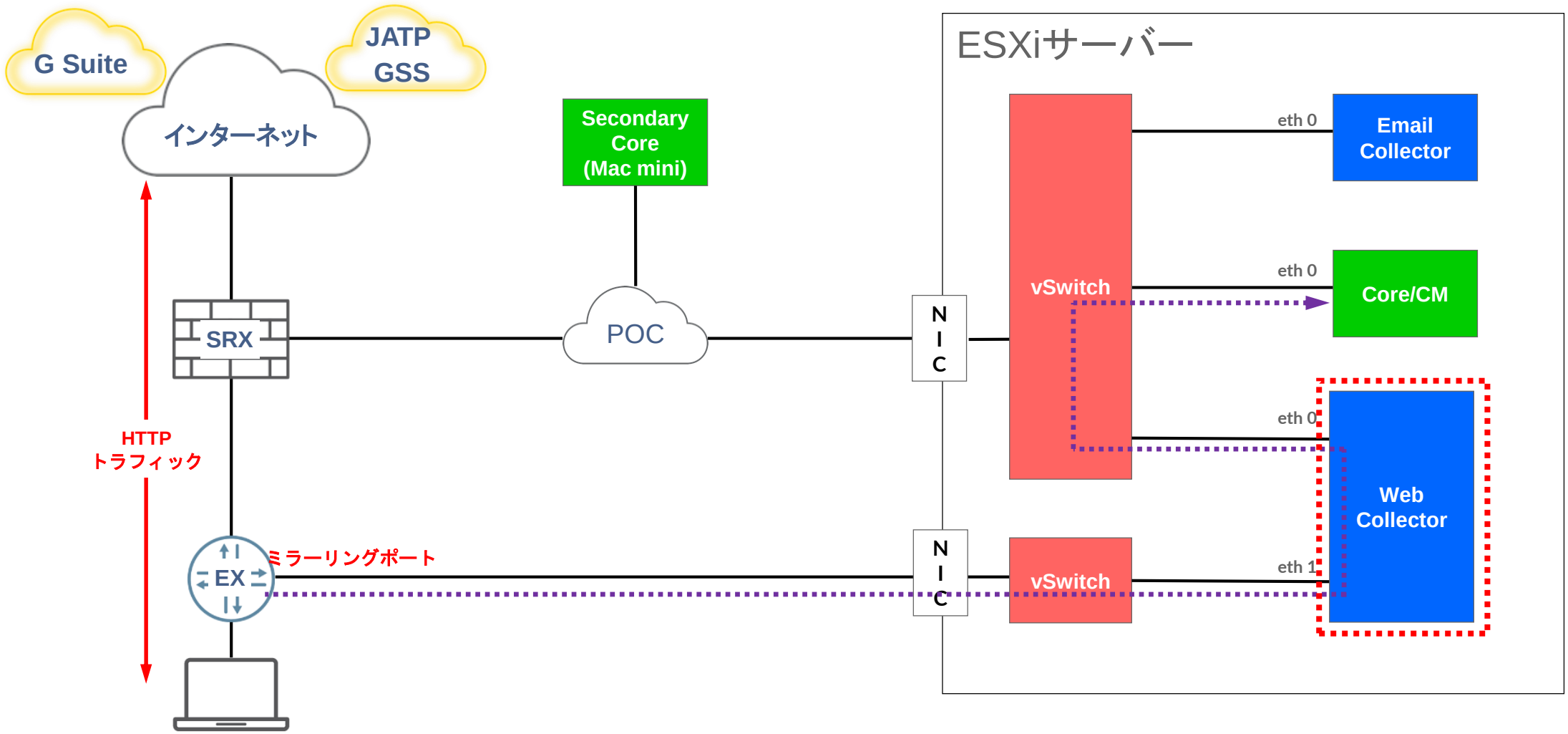
アジェンダ

- 仮想サーバー設定手順(OVAファイル)
- 仮想サーバー設定手順(OVFファイル)
- Web Collector動作確認手順
- Web Collectorコマンド一例

© 2019 Juniper Networks

Juniper Business Use Only

構成イメージ



© 2019 Juniper Networks

Juniper Business Use Only

仮想サーバー設定手順
OVAファイル

仮想サーバーの設定について

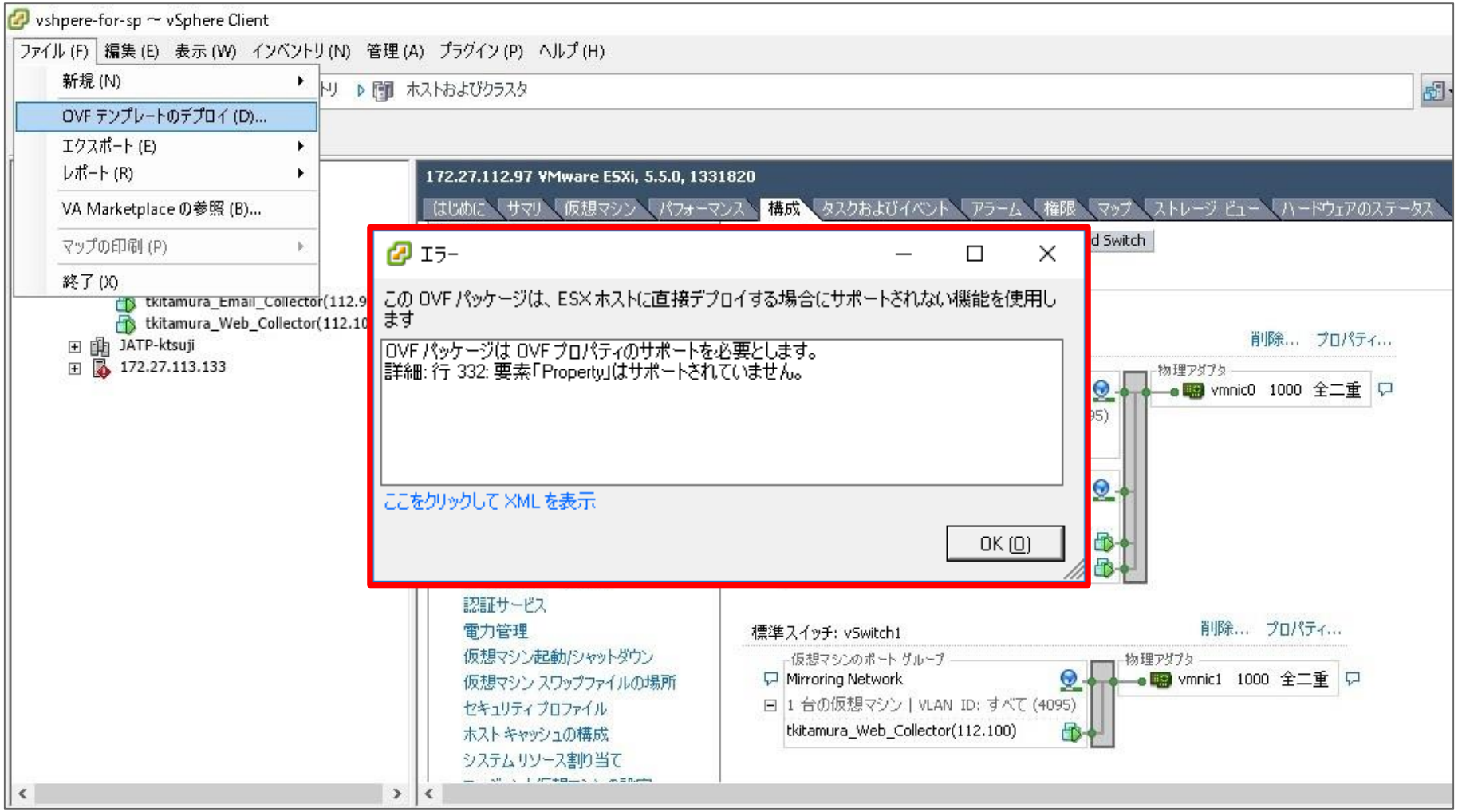
- 仮想サーバーの設定には以下の２通りの方法があります。
  - OVAファイルのデプロイ(※vCenter Serverが必要)
    ⇒次ページ以降を参照
  - OVFファイルのデプロイ
    ⇒仮想サーバー設定手順(OVFファイル)を参照

© 2019 Juniper Networks
Juniper Business Use Only

仮想サーバー設定手順(OVAファイル)

© 2019 Juniper Networks

仮想サーバー設定手順(OVAファイル)
エラー表示一例



© 2019 Juniper Networks

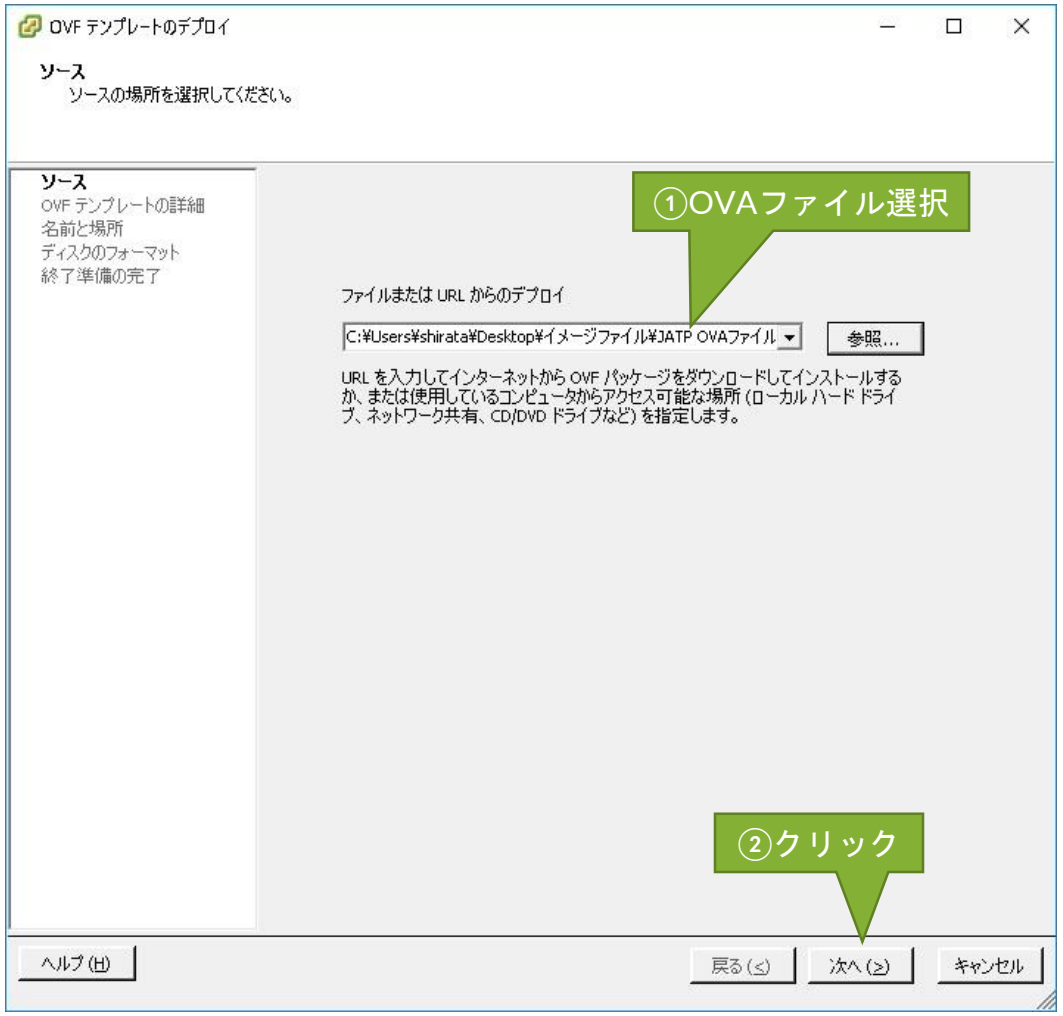
Juniper Business Use Only

仮想サーバー設定手順(OVAファイル)

© 2019 Juniper Networks

Juniper Business Use Only

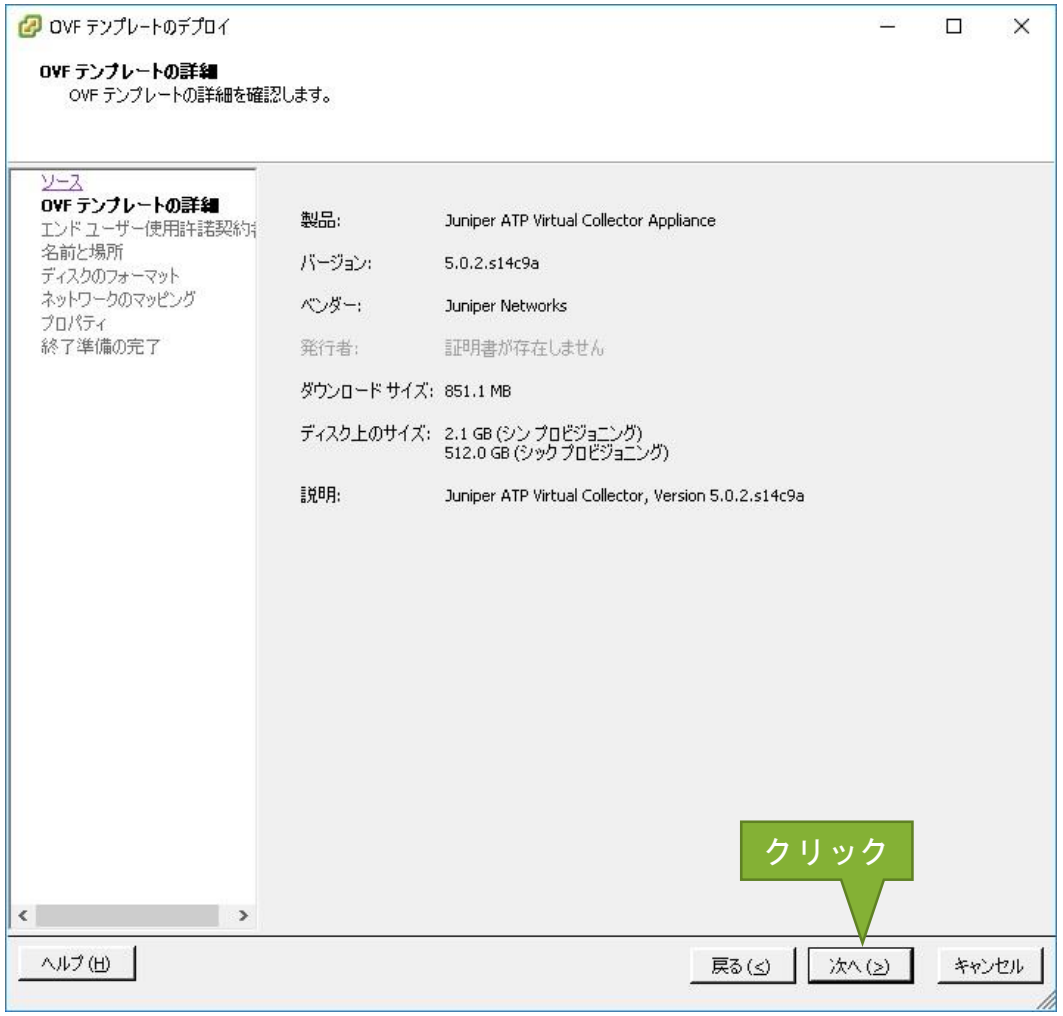
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

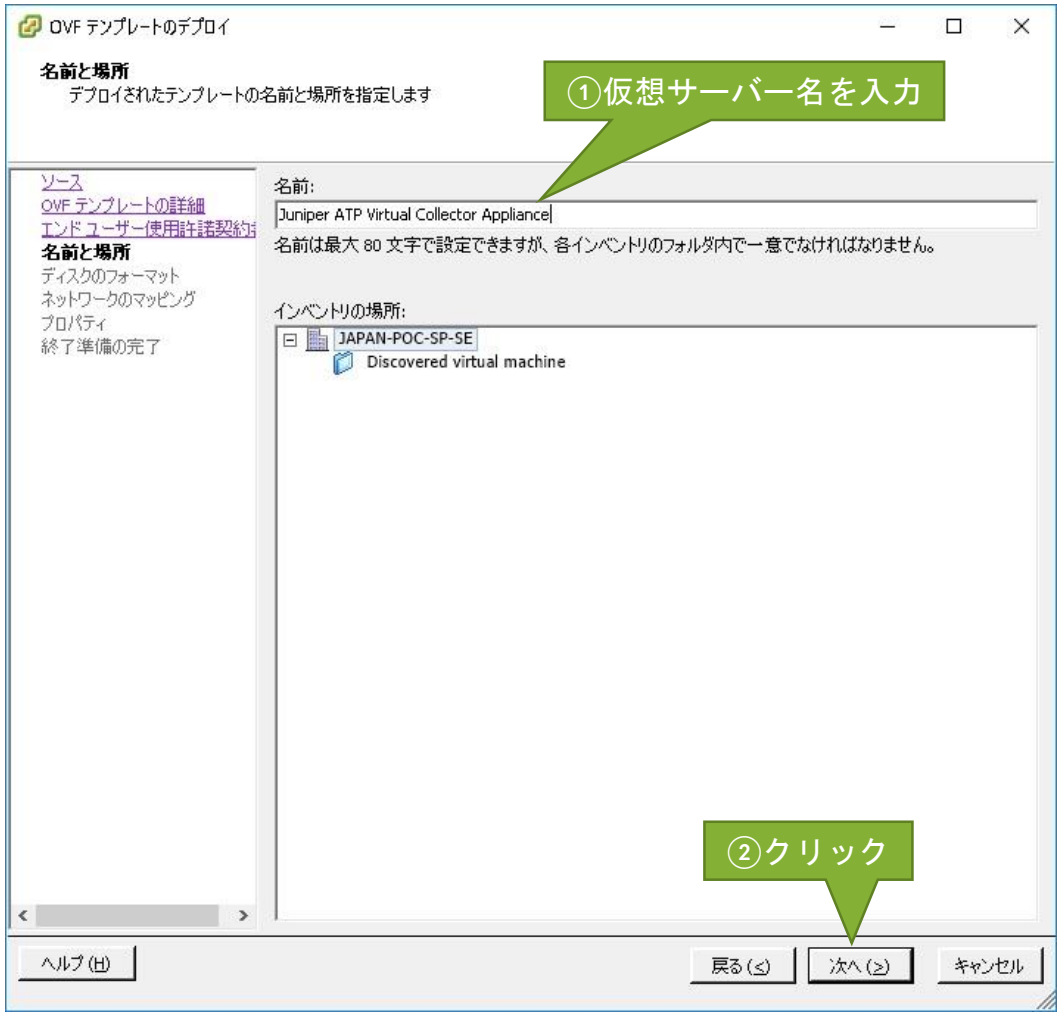
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

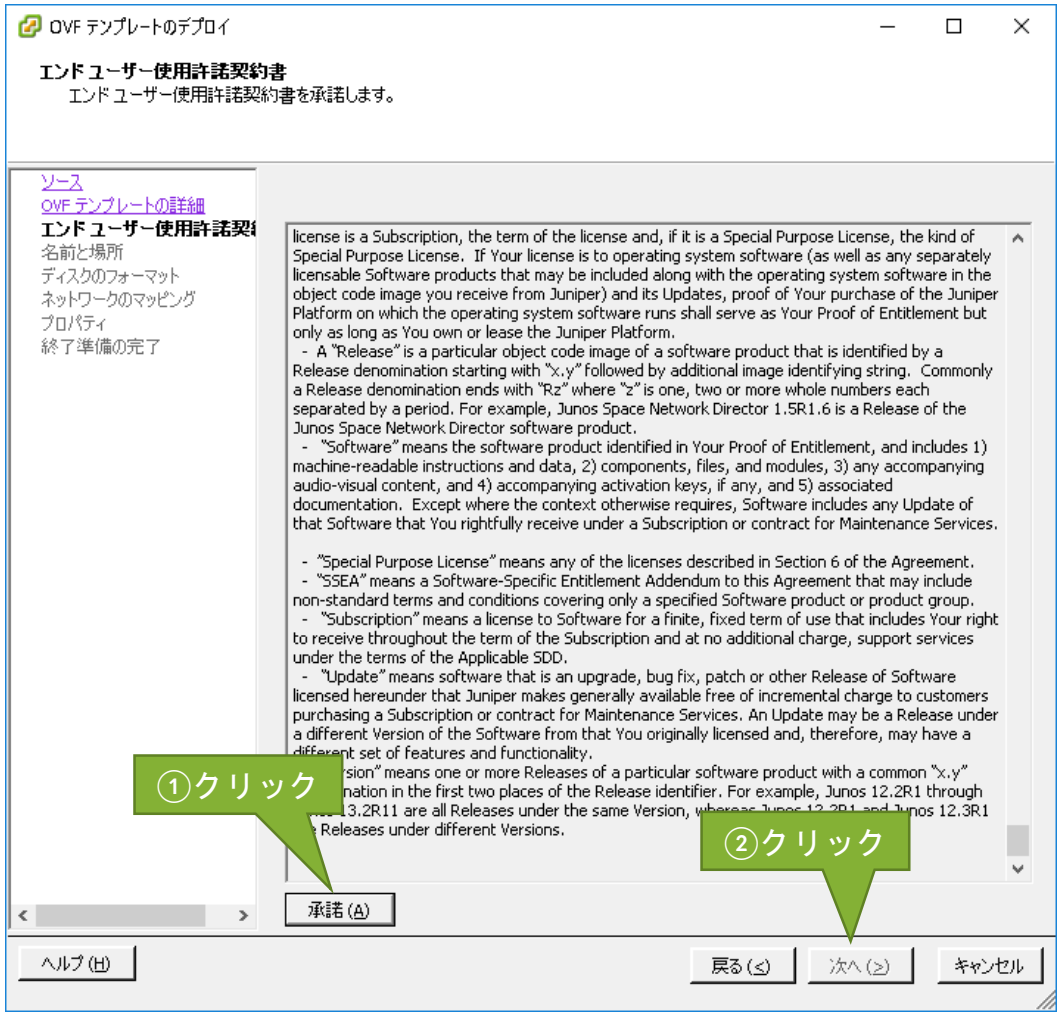
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

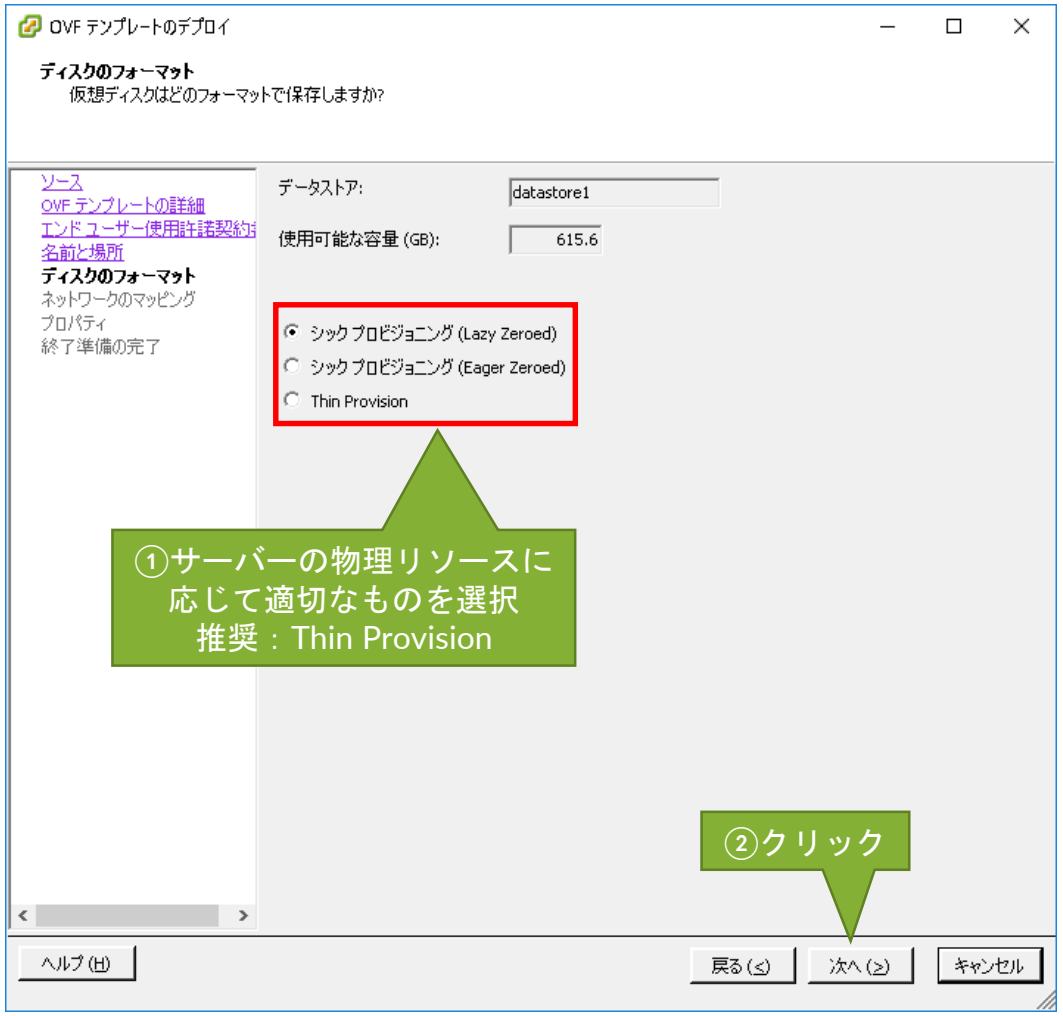
Juniper Business Use Only

仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

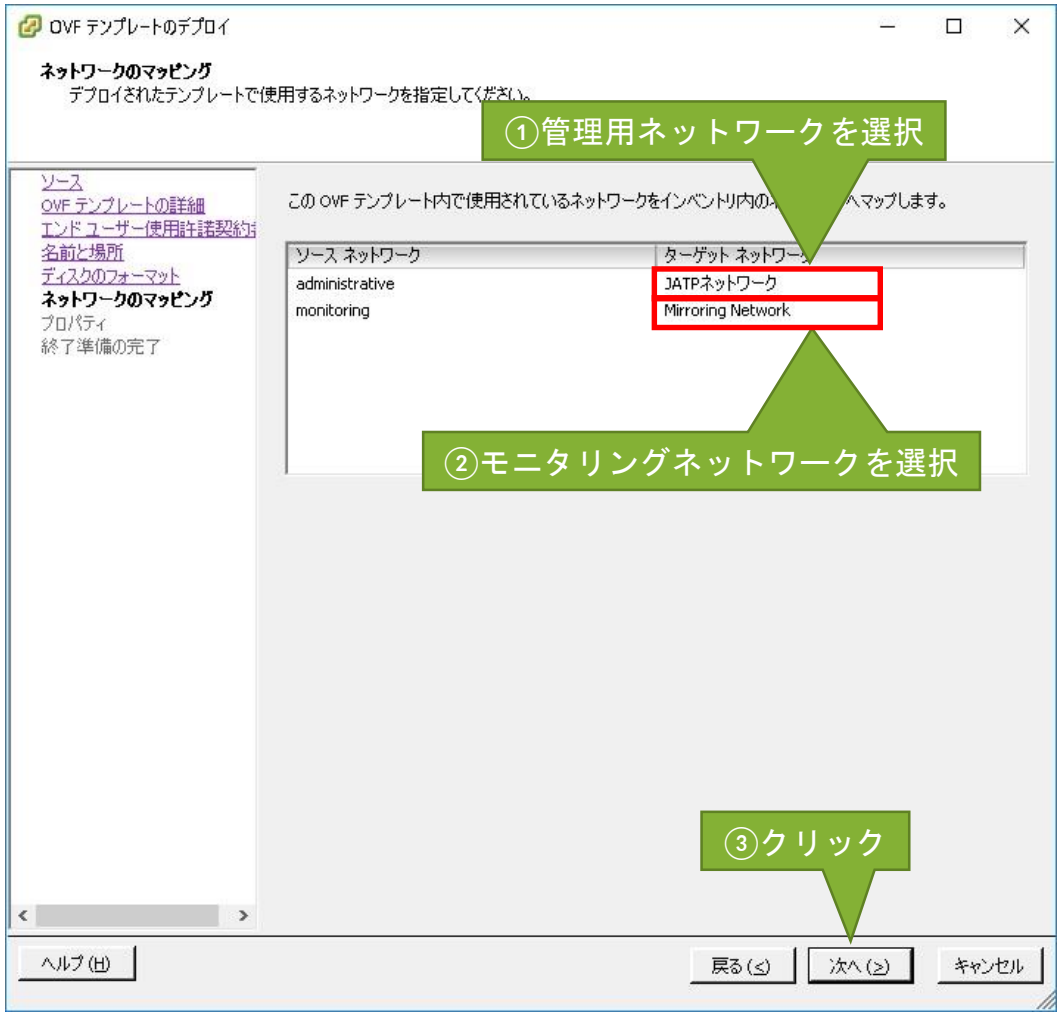
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

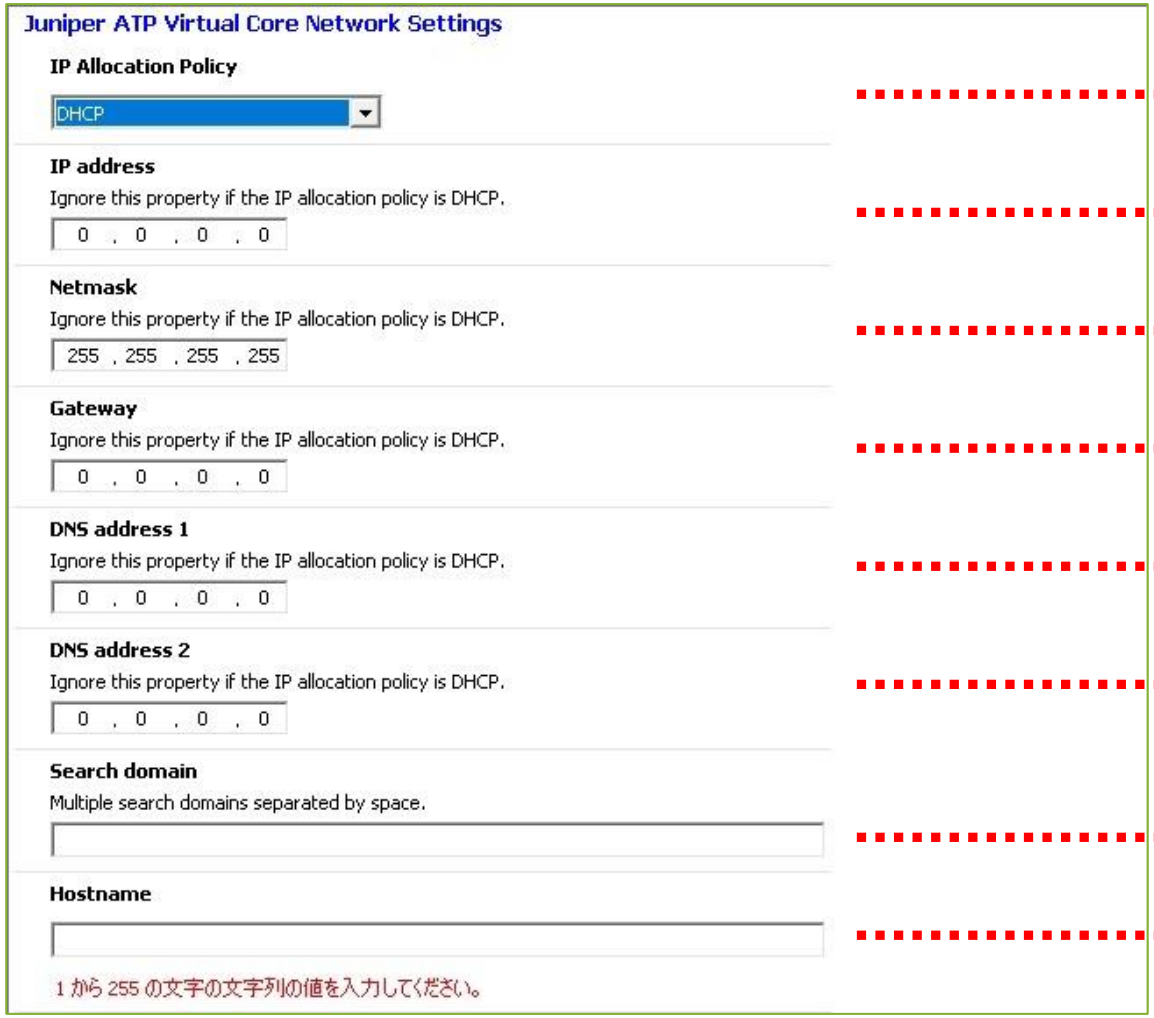
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

仮想サーバー設定手順(OVAファイル)



DHCP / Staticを選択

仮想サーバーのIPアドレスの設定

サブネットマスクの設定

ゲートウェイの設定

DNS1の設定

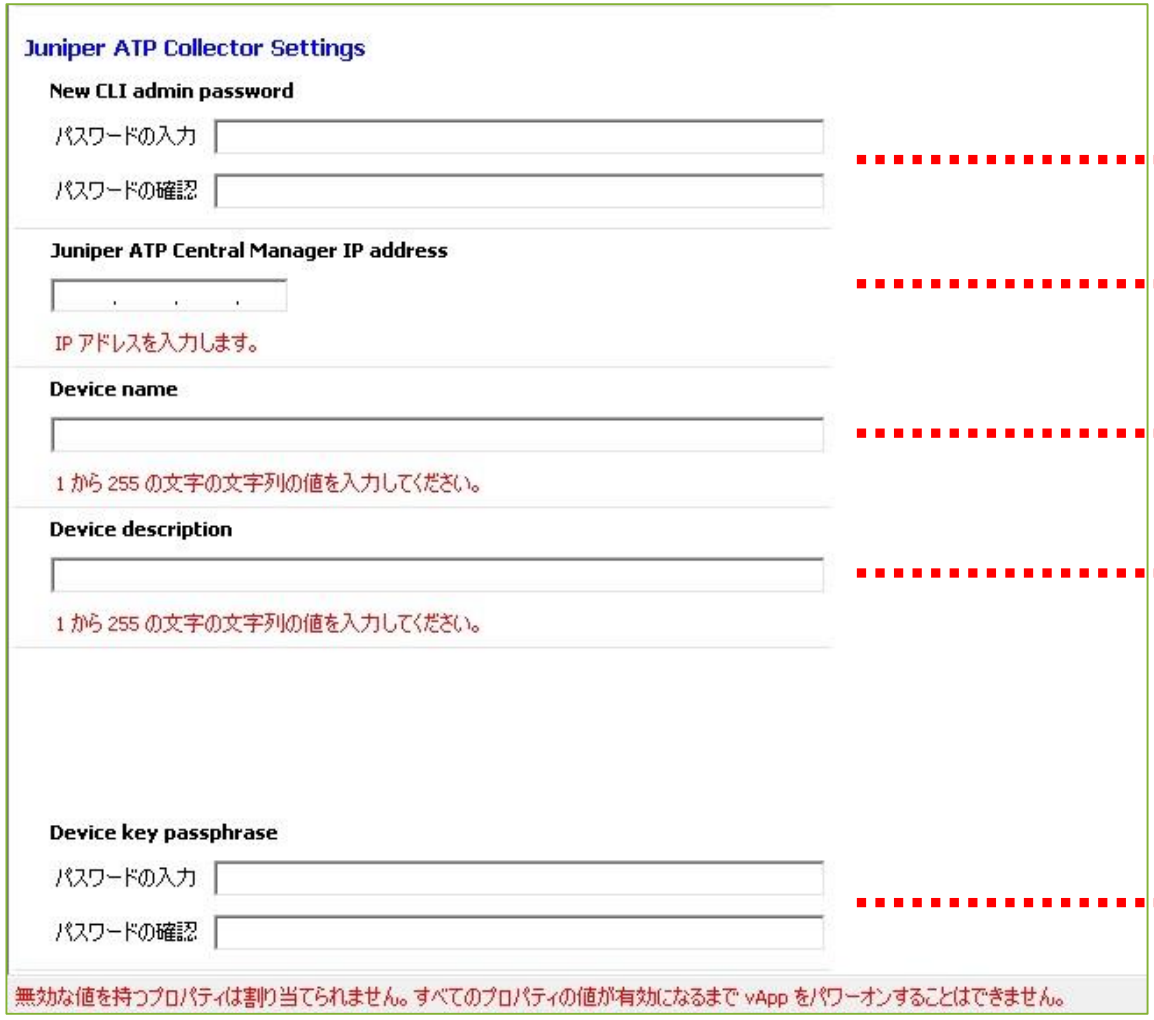
DNS2の設定(任意)

検索用ドメイン名の設定(任意)

サーバーのホストネームの設定

© 2019 Juniper Networks

仮想サーバー設定手順(OVAファイル)



adminログインパスワードの設定

Core/CMのIPアドレスを入力

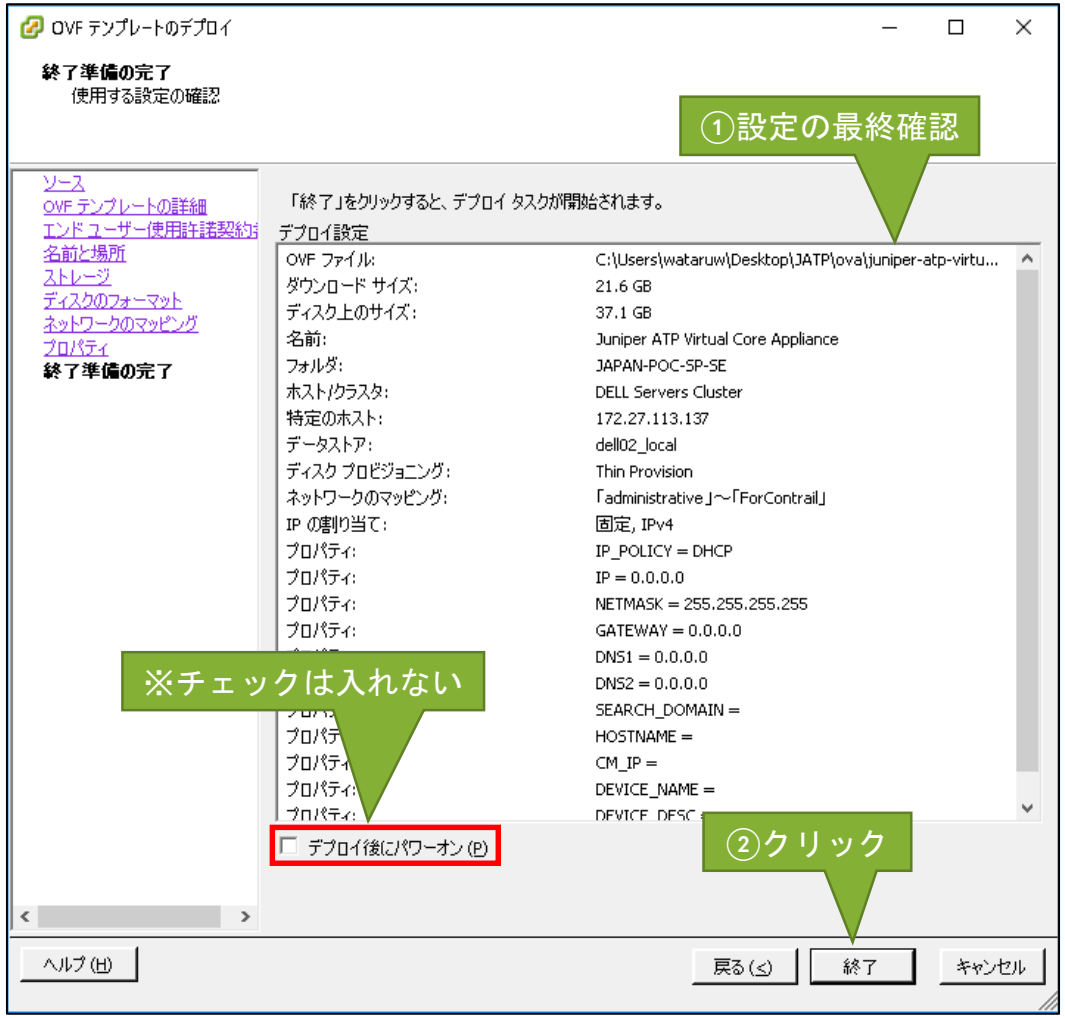
デバイスネームの設定

デバイスの説明

接続するCore,Collectorで
すべて共通の値を入力

© 2019 Juniper Networks

仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

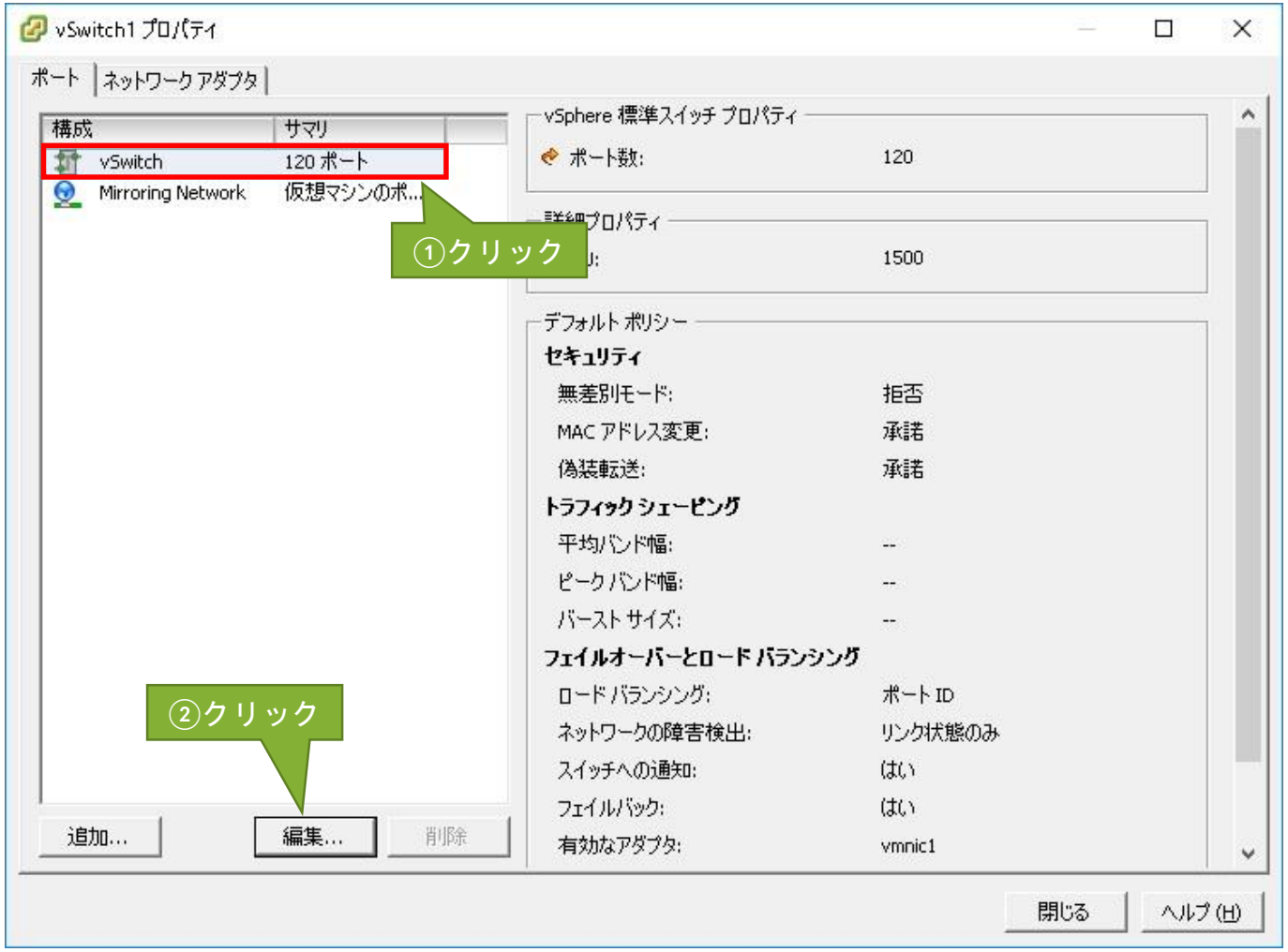
Juniper Business Use Only

仮想サーバー設定手順(OVAファイル)

© 2019 Juniper Networks

Juniper Business Use Only

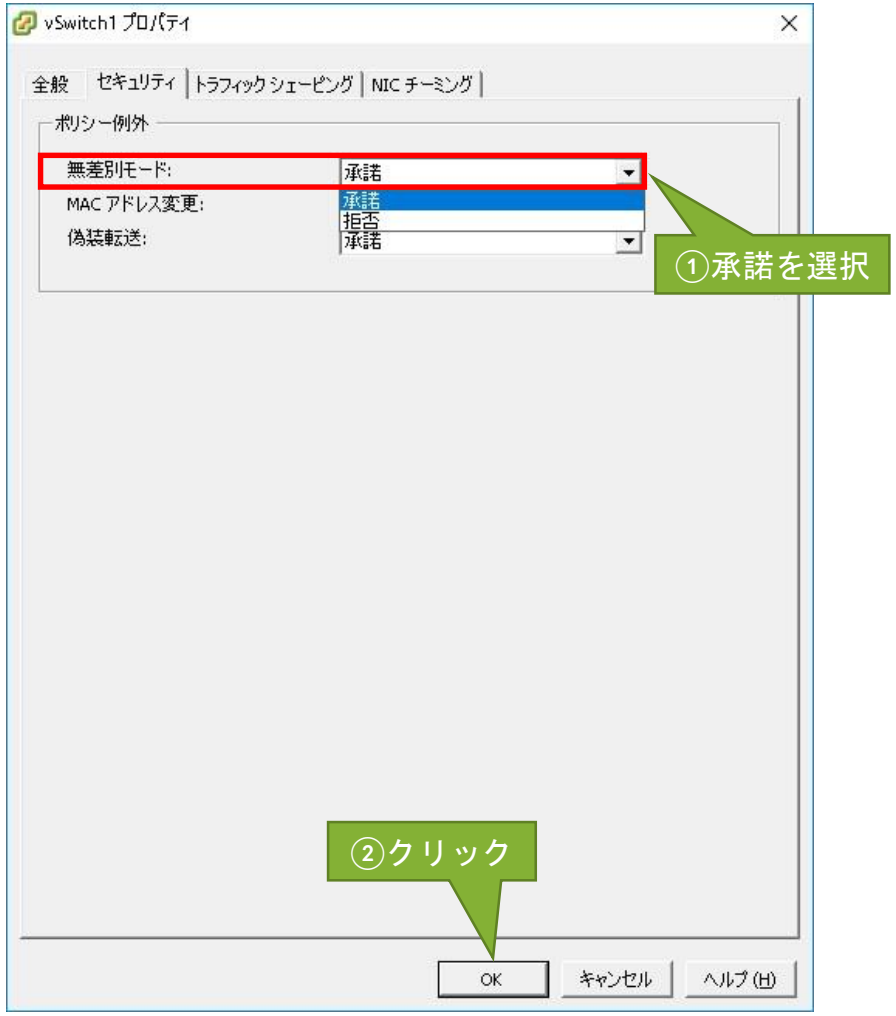
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

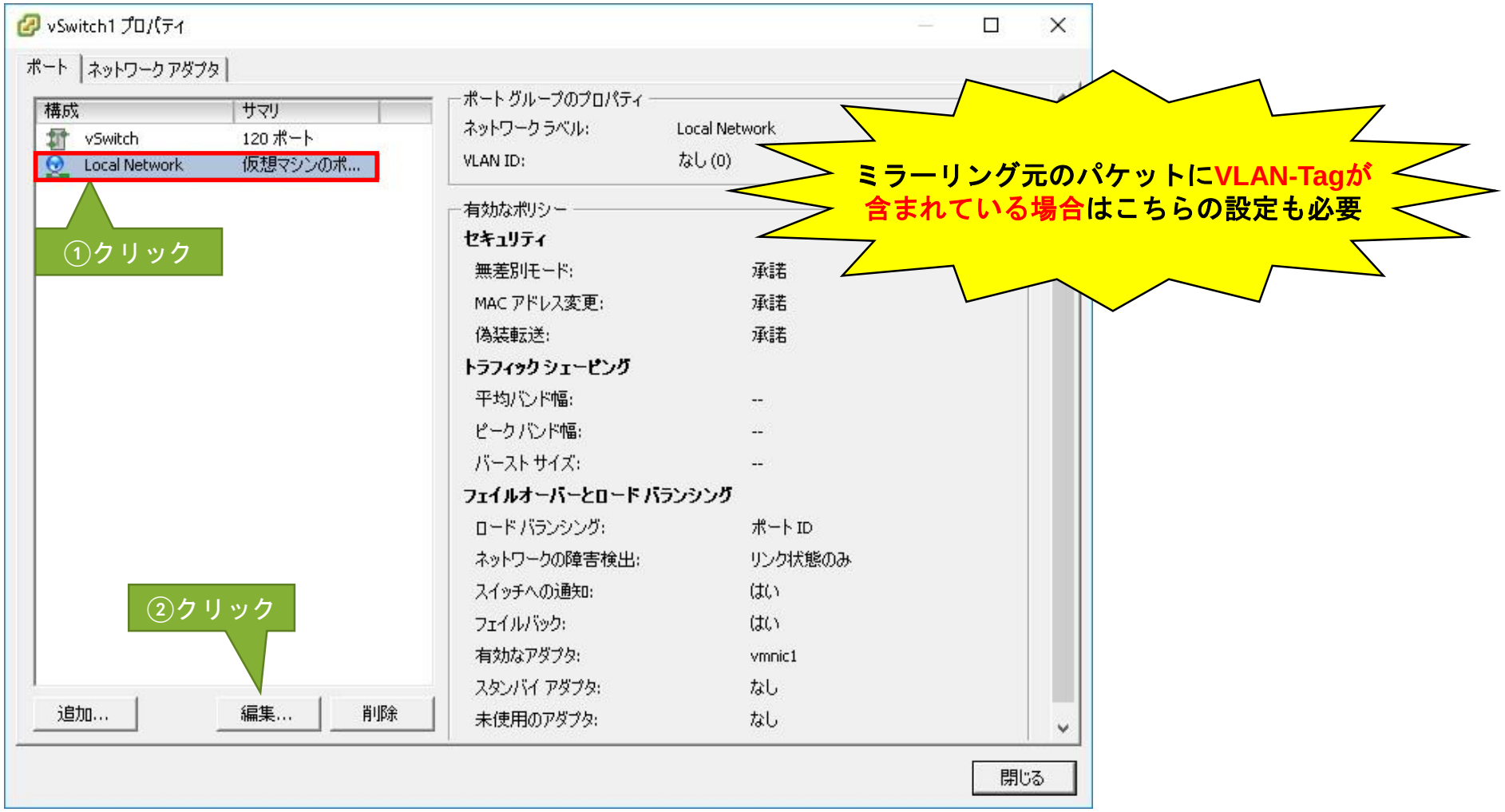
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

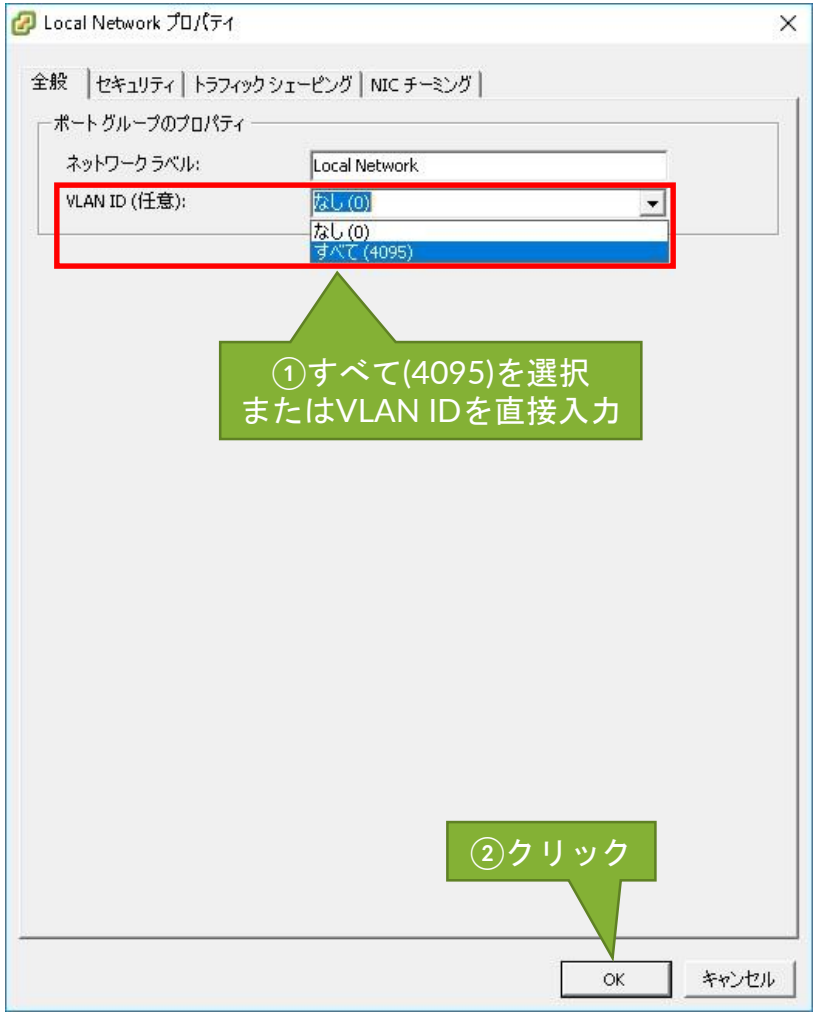
仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

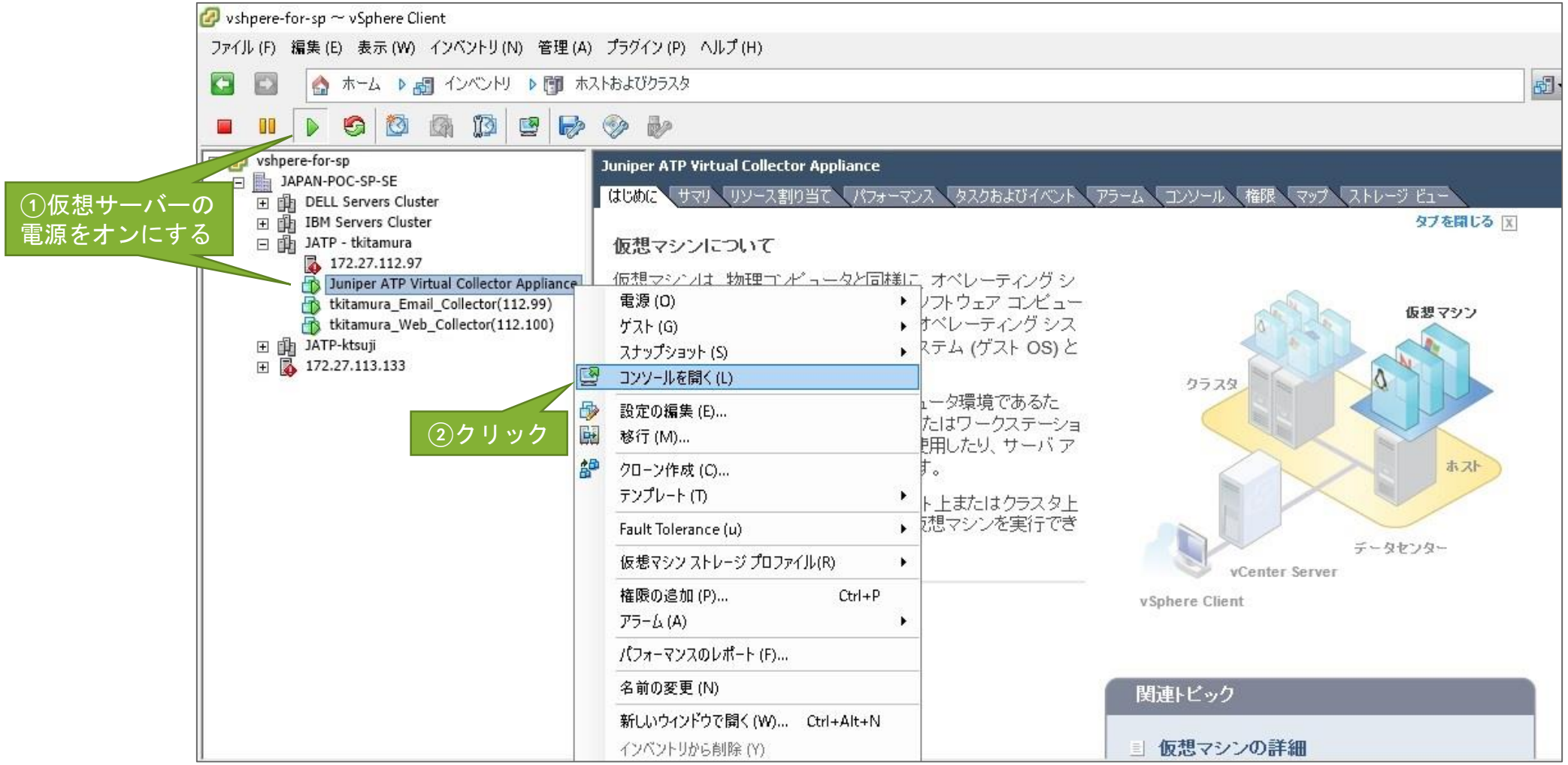
Juniper Business Use Only

仮想サーバー設定手順(OVAファイル)



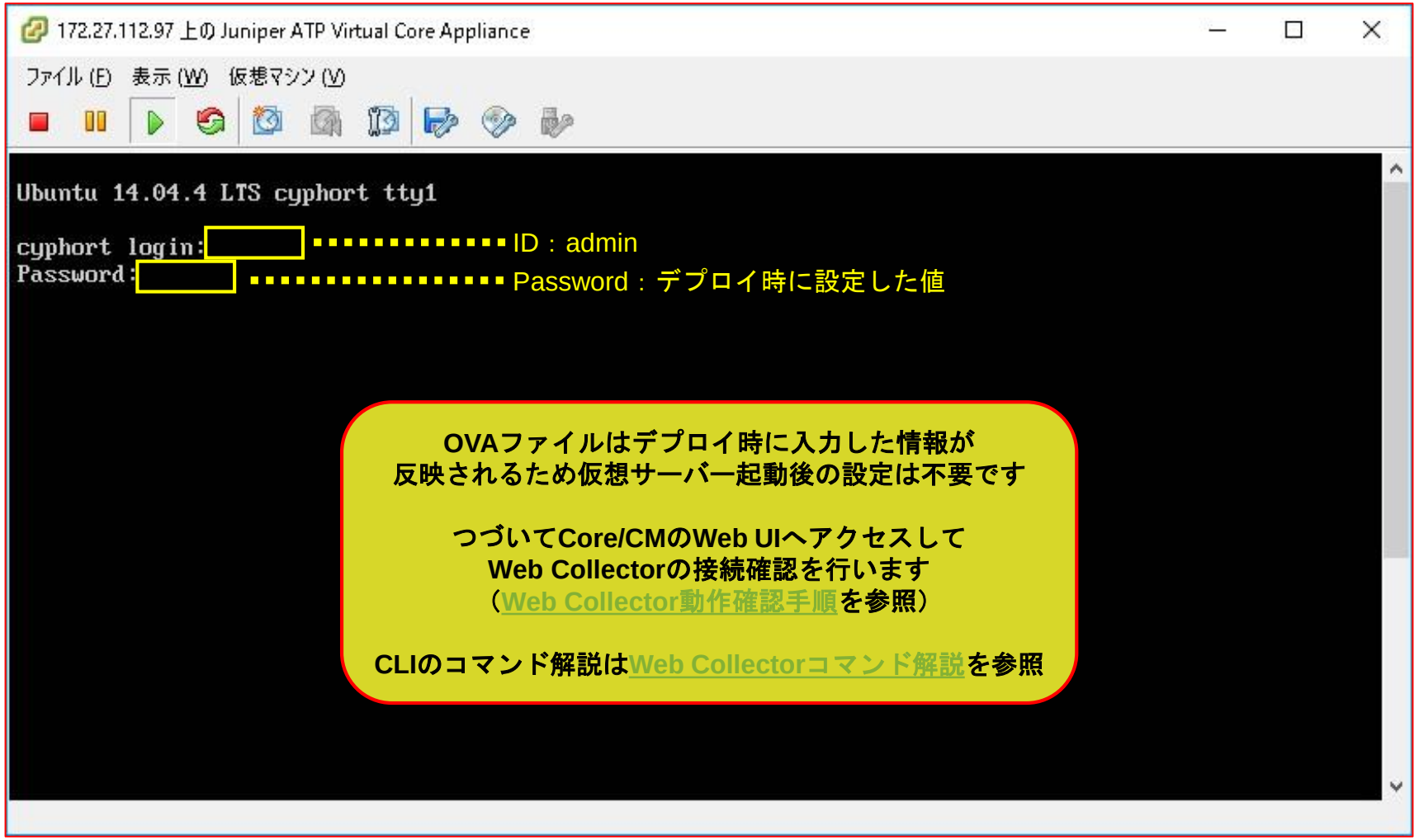
© 2019 Juniper Networks

仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

仮想サーバー設定手順(OVAファイル)



© 2019 Juniper Networks

Juniper Business Use Only

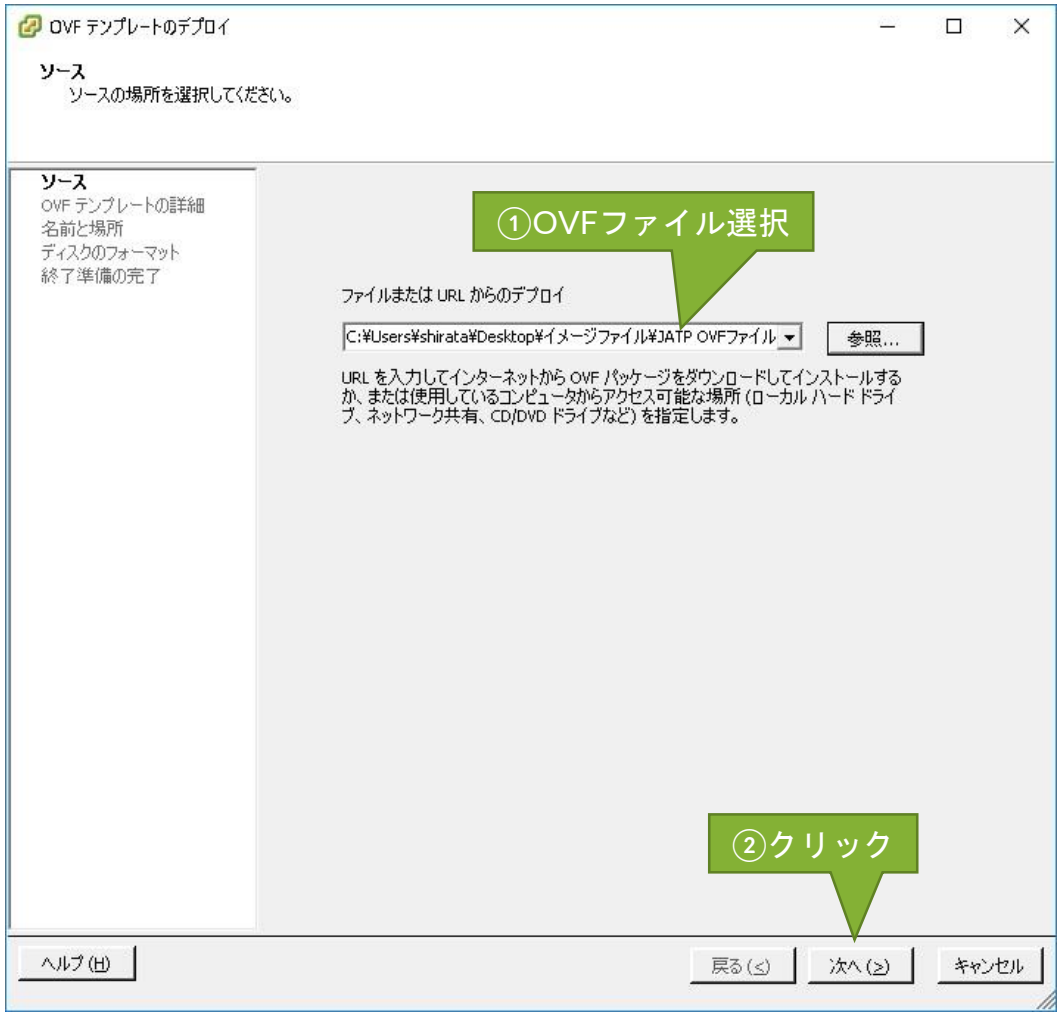
仮想サーバー設定手順
OVFファイル

仮想サーバー設定手順(OVFファイル)

© 2019 Juniper Networks

Juniper Business Use Only

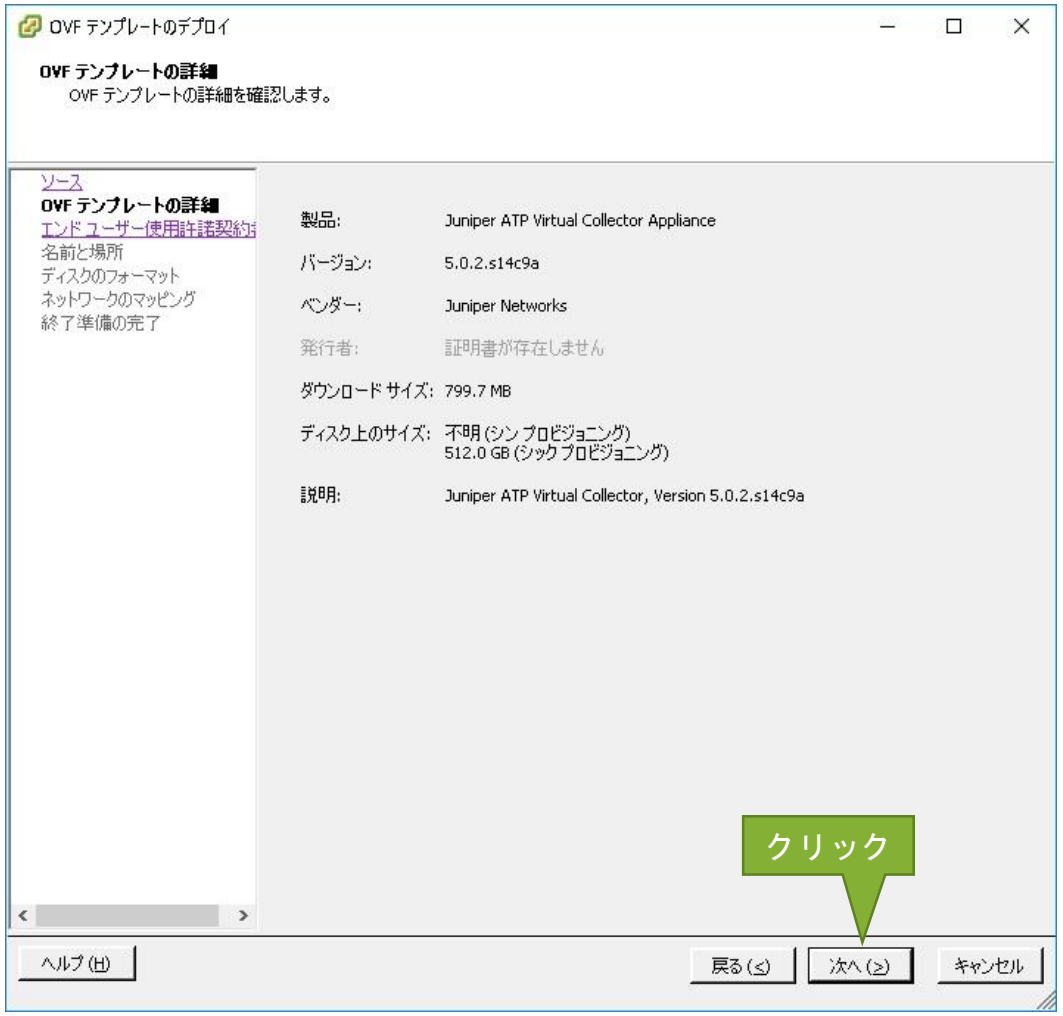
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

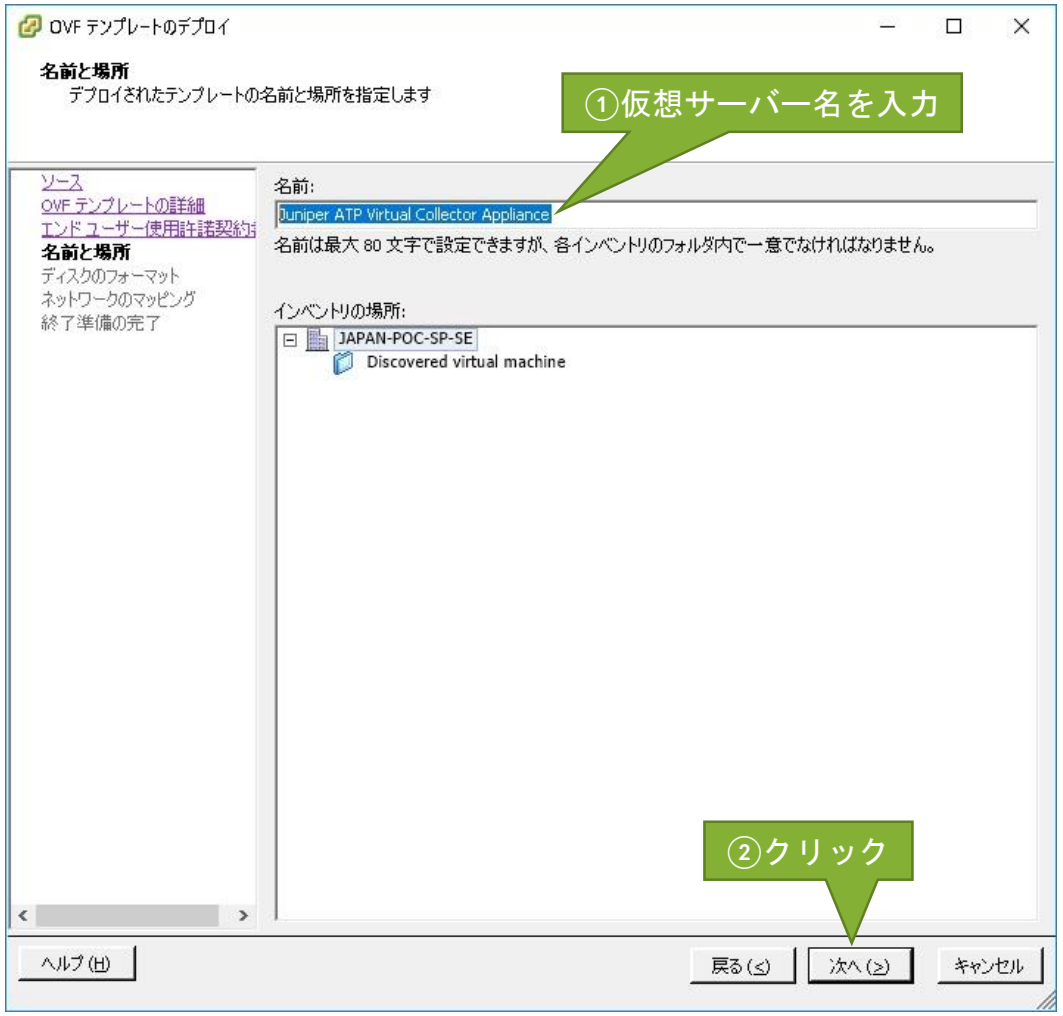
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

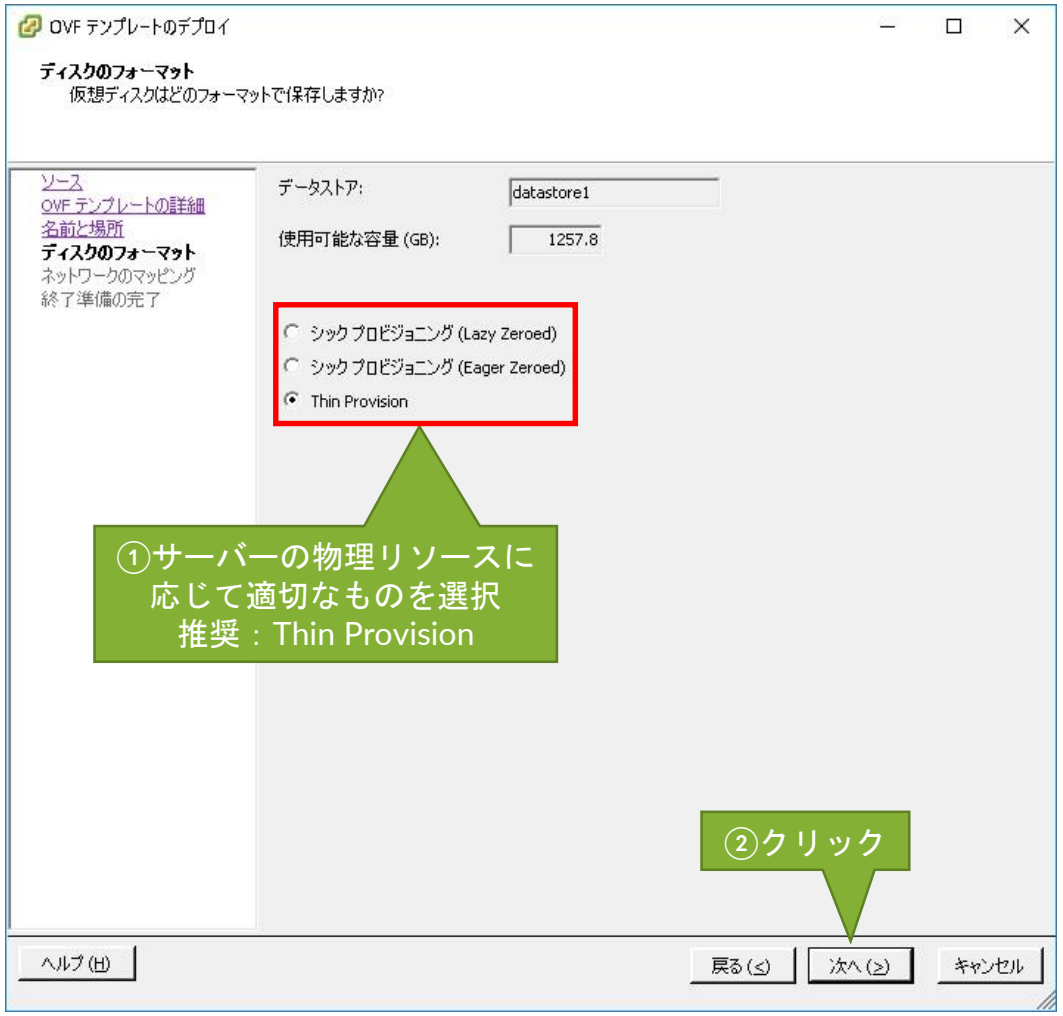
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

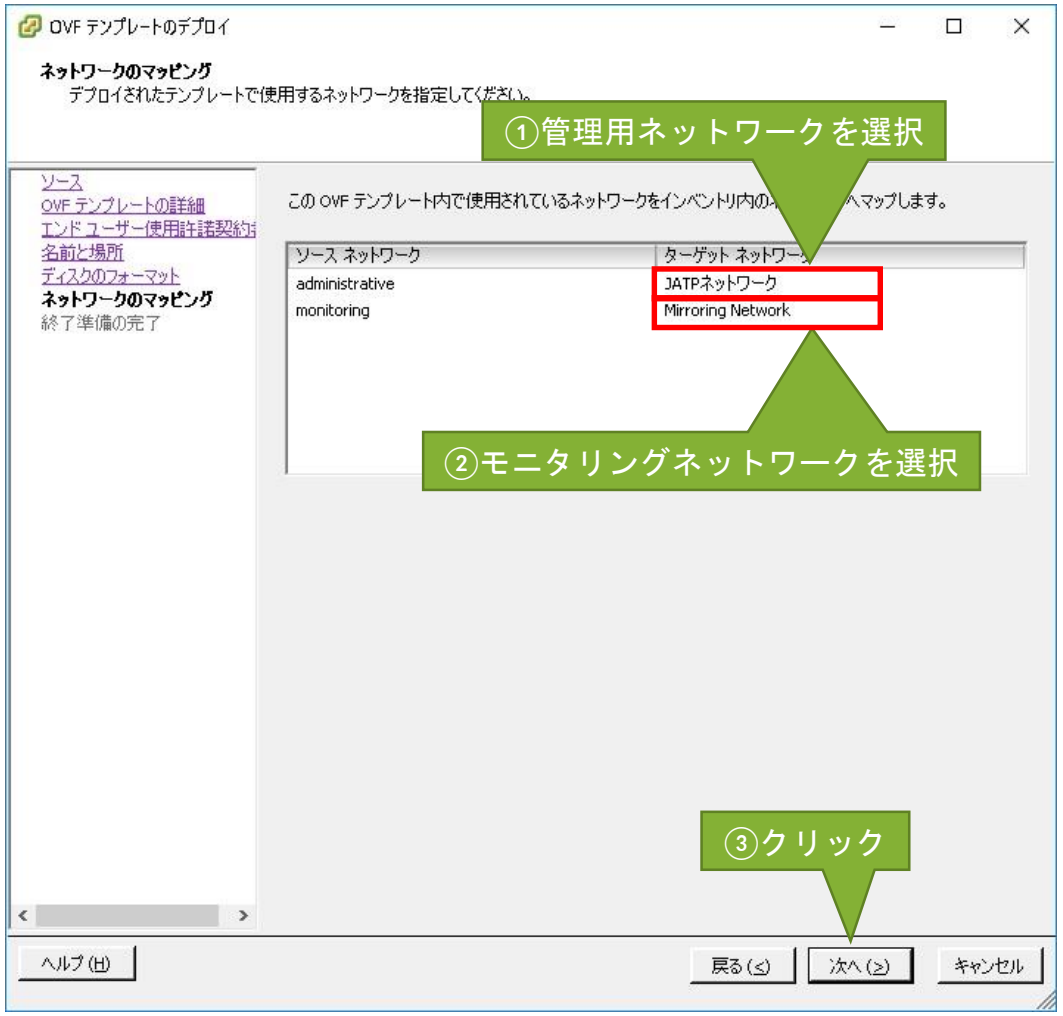
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

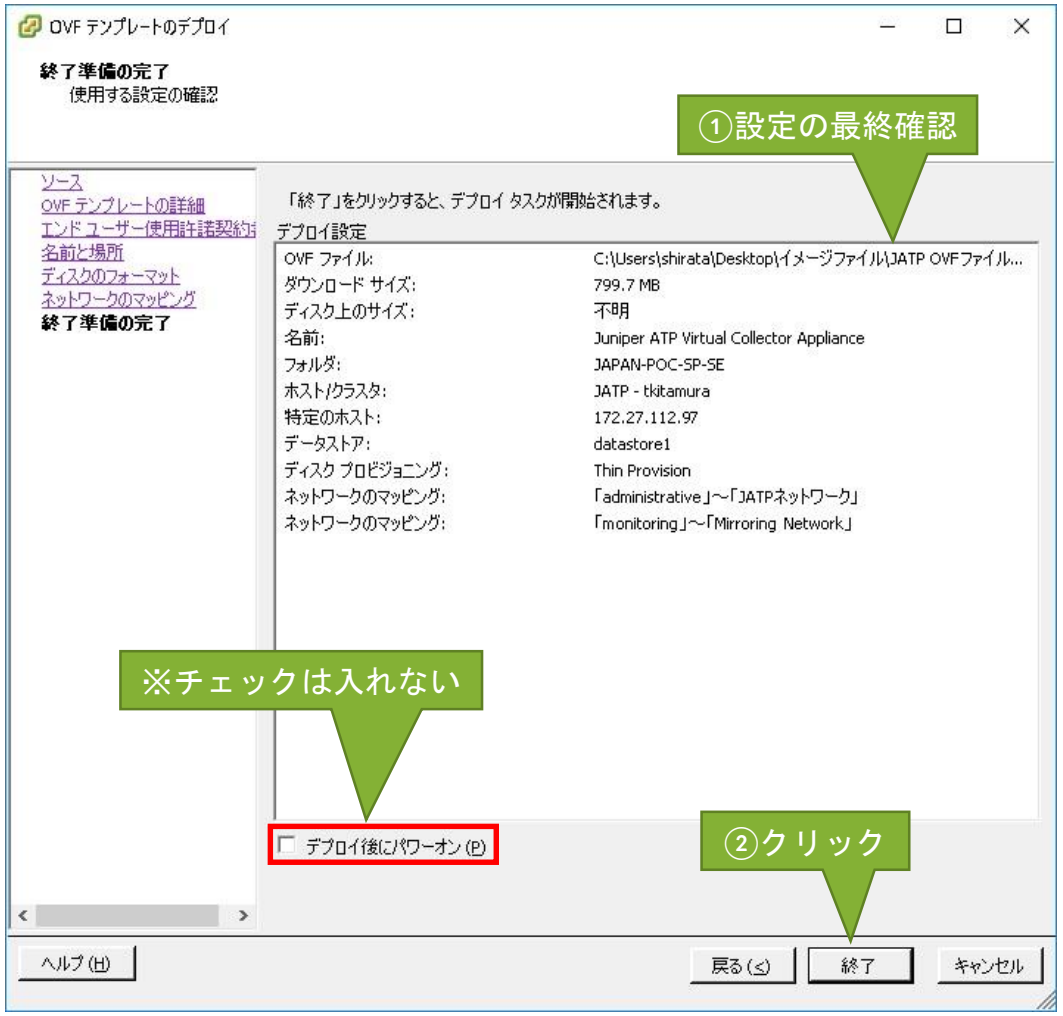
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

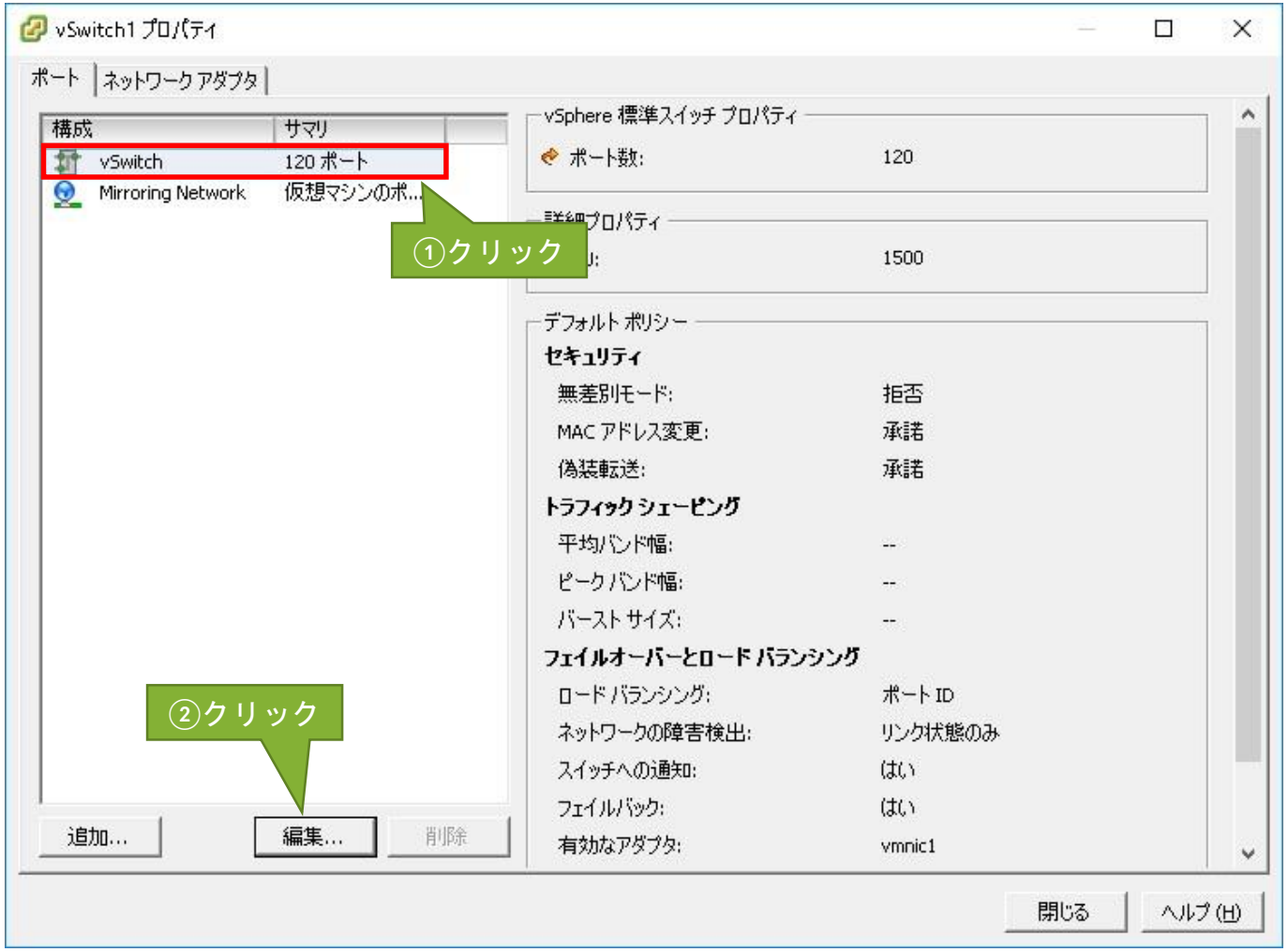
Juniper Business Use Only

仮想サーバー設定手順(OVFファイル)

© 2019 Juniper Networks

Juniper Business Use Only

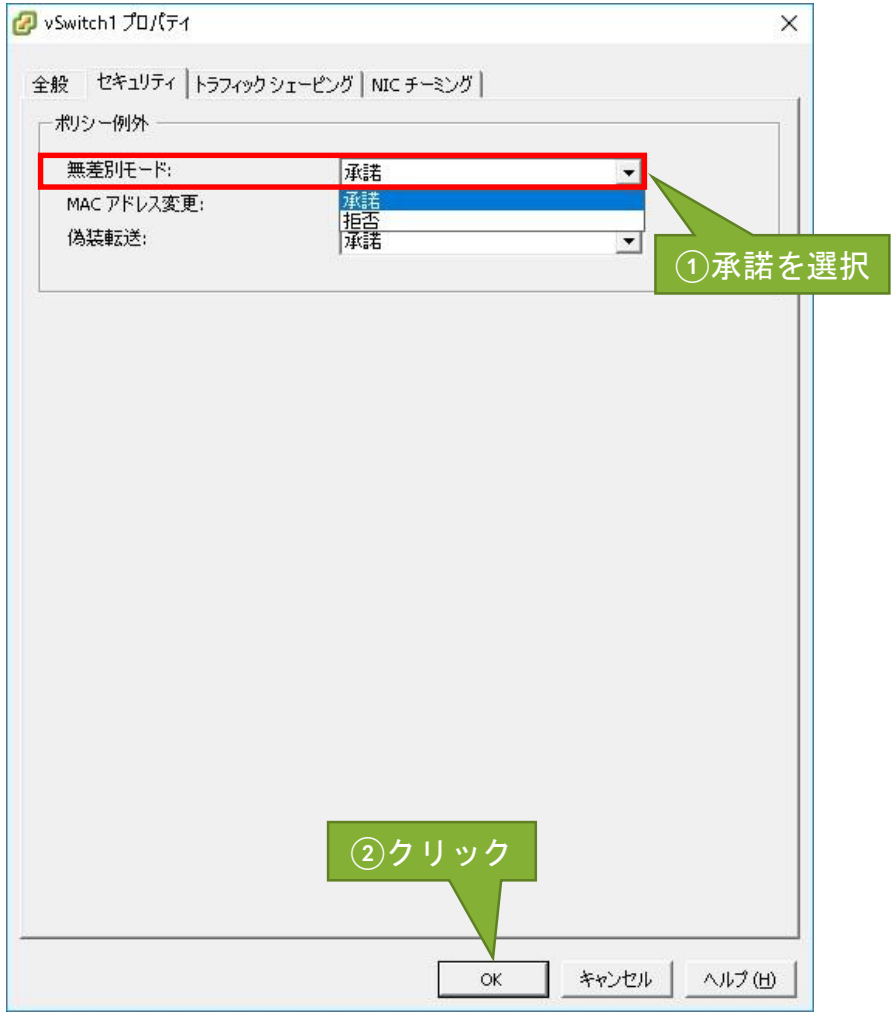
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

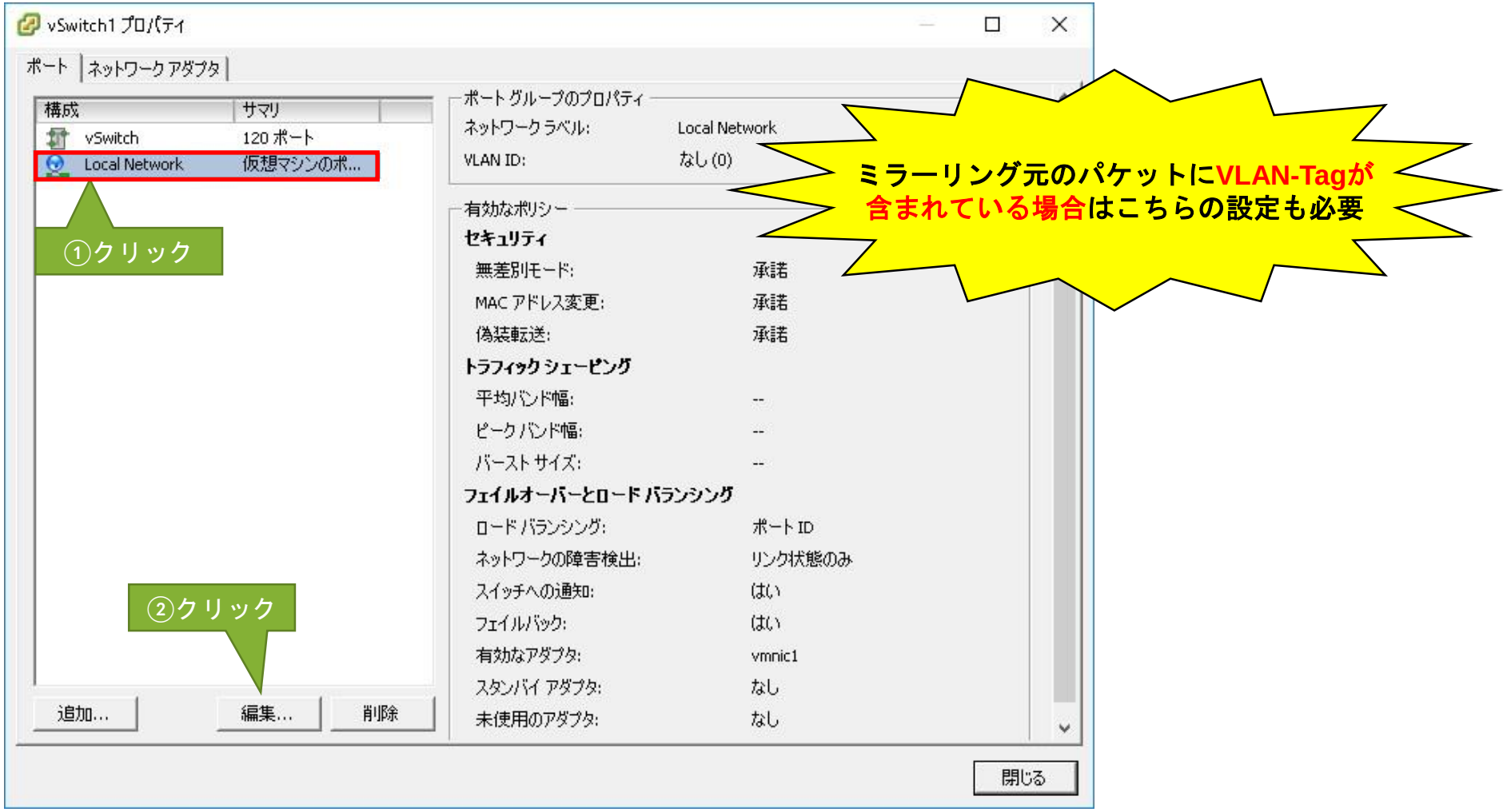
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

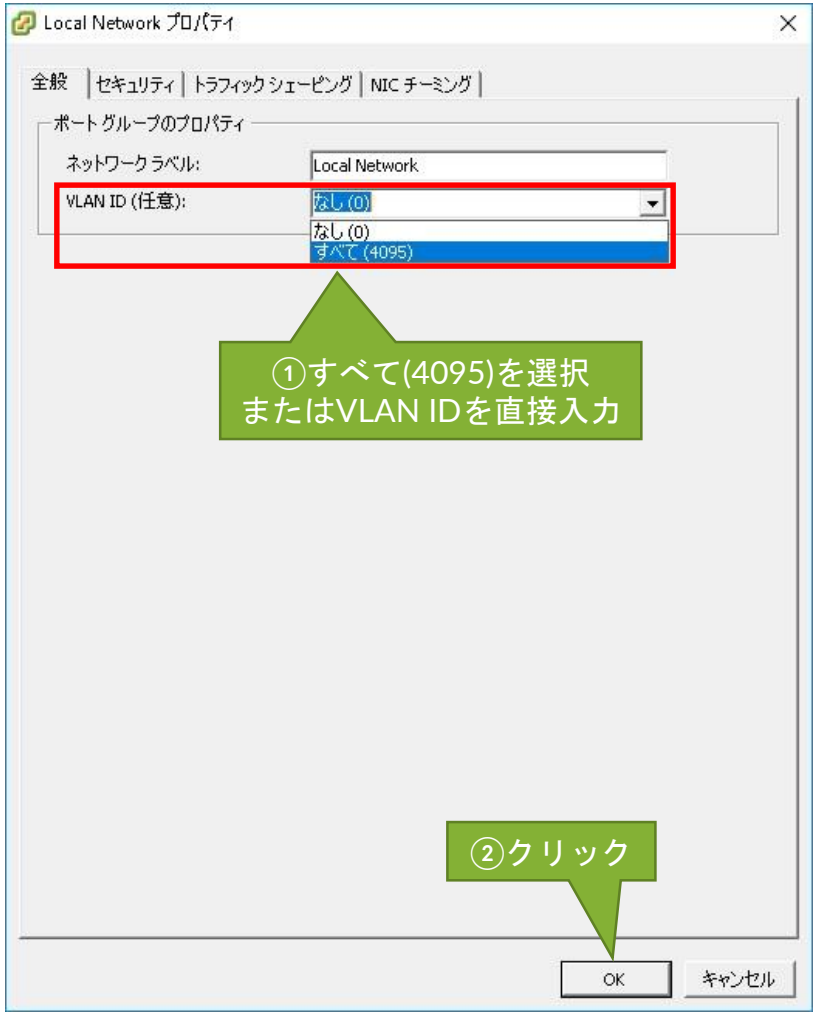
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

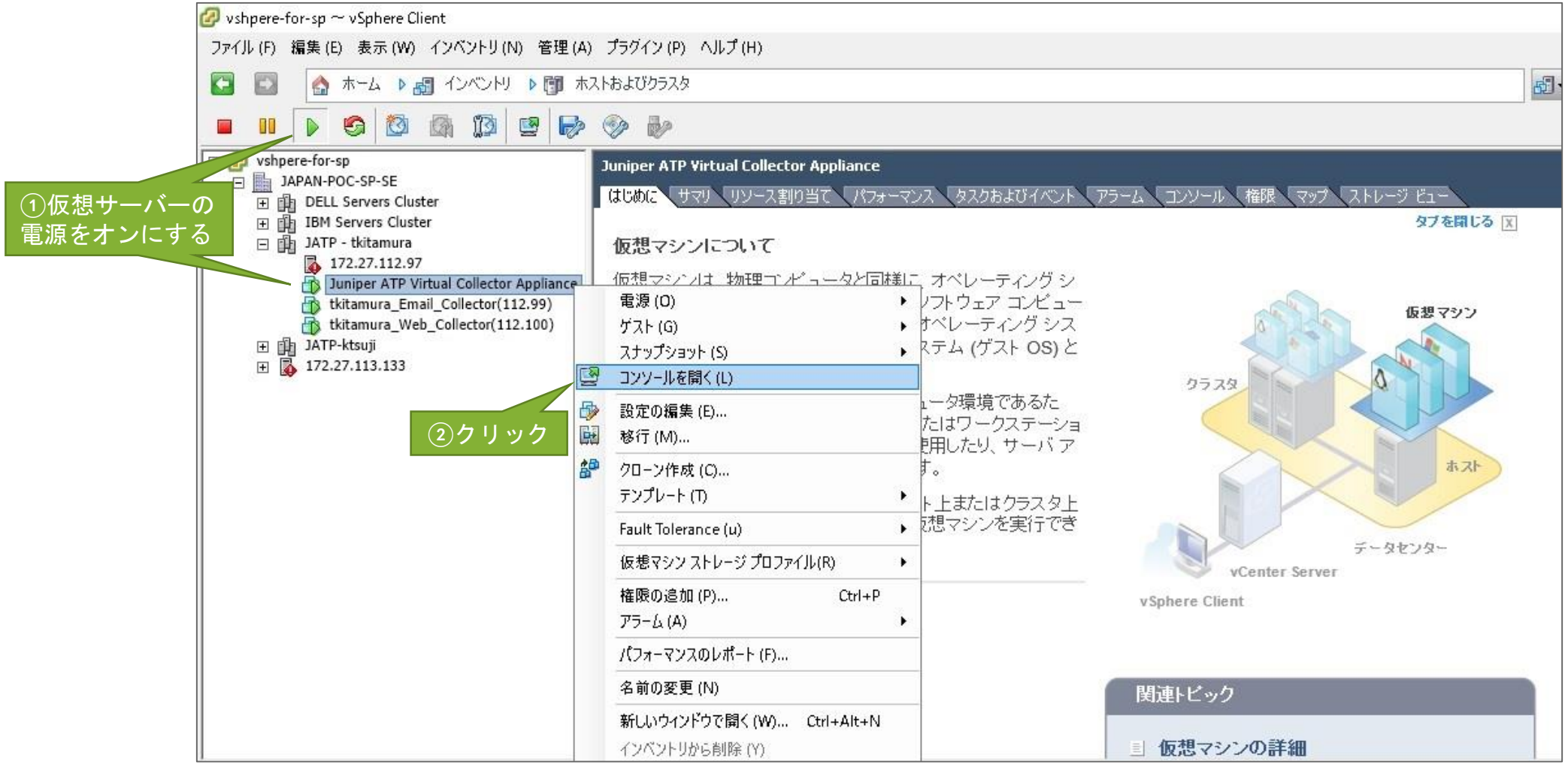
Juniper Business Use Only

仮想サーバー設定手順(OVFファイル)



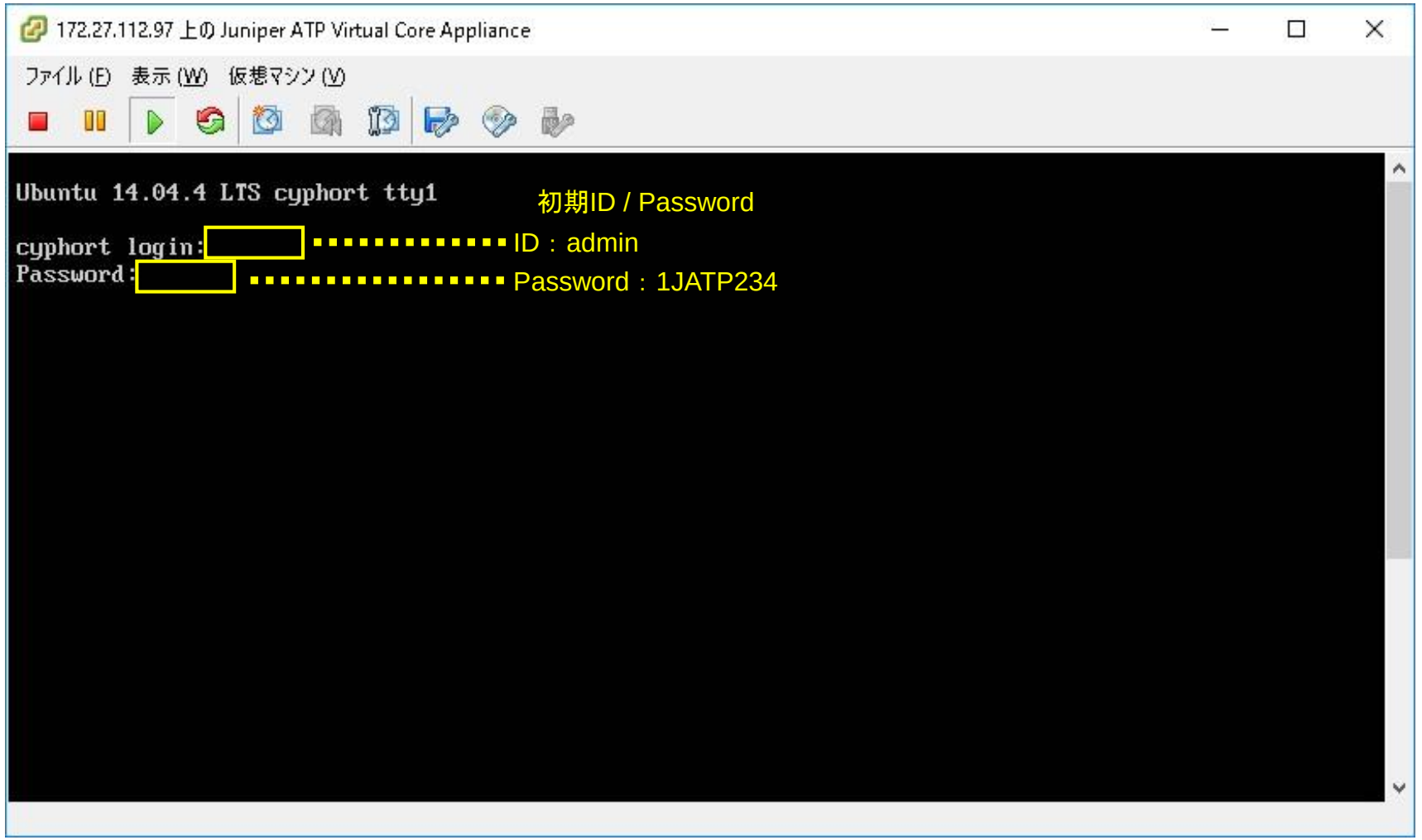
© 2019 Juniper Networks

仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

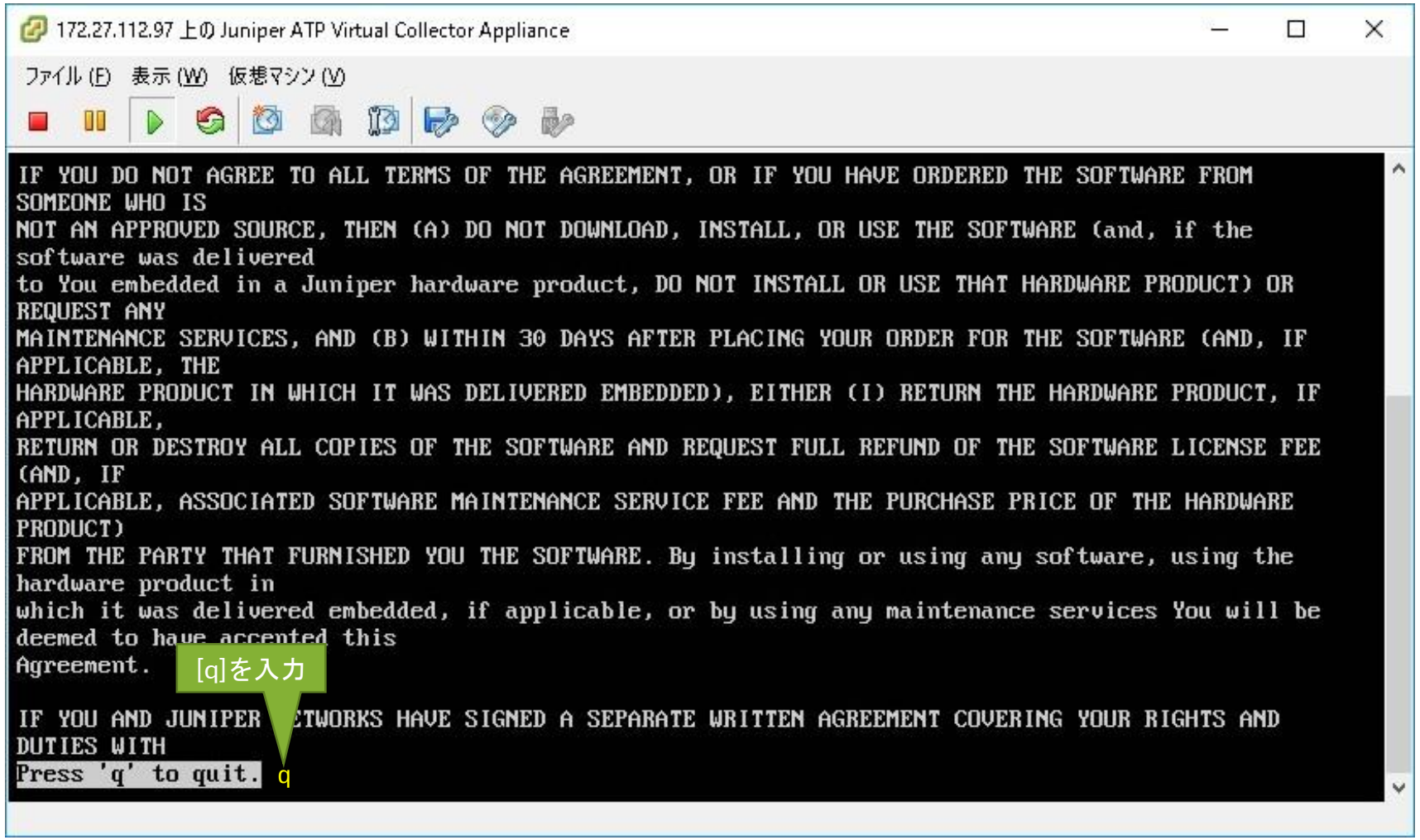
仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

Juniper Business Use Only

仮想サーバー設定手順(OVFファイル)



© 2019 Juniper Networks

仮想サーバー設定手順(OVFファイル)

```
**********************************************************************
*      Juniper Networks Advanced Threat Prevention Appliance         *
*                                                                    *
**********************************************************************

Do you accept the End-user License Agreement (Yes/No)?  yes


The CLI admin password needs to be changed from the default.
Enter the new password of CLI admin:  新規のパスワードを入力
The entered password ********: it is based on a dictionary word.
Use this password anyway? (Yes/No)?  yes
Retype the new password of CLI admin:  再度同じパスワードを入力
```

© 2019 Juniper Networks

仮想サーバー設定手順(OVFファイル)

```
**********************************************************************
*      Juniper Networks Advanced Threat Prevention Appliance         *
*                                                                    *
**********************************************************************

Do you want to configure the system by using the configuration wizard (Yes/No)?  yes / no
（※wizardを使用せずに個別に設定・変更することも可能）

****** Setting the IP address and Domain Name Servers ******
Use DHCP to obtain the IP address and DNS server address for the management (eth0) interface (Yes/No)?  yes / no
Enter IP address for this management (eth0) interface:  管理用IPアドレスを入力
Enter netmask for this management (eth0) interface:  サブネットマスクを入力
Enter gateway IP Address for this management (eth0) interface:  デフォルトゲートウェイのIPアドレス入力
Enter primary DNS server IP Address for the management (eth0) interface:  DNSサーバーのアドレスを入力
Do you have a secondary DNS server for the management (eth0) interface? (Yes/No)?  yes / no （任意）
Do you want to enter the search domains for management (eth0) interface? (Yes/No)?  yes / no （任意）
Restart the management (eth0) interface (Yes/No)?  yes

****** Setting the device host name ******
Please enter a valid hostname: ホスト名を入力
Regenerate the SSL self-signed certificate? (Yes/No)? yes / no

****** Setting the device basic attributes ******
Please enter the following server attributes...
Is this a Central Manager device (Yes/No)? No
Central Manager IP address: Core/CMのIPアドレスを入力
Device name: デバイス名を入力（Web UI上の表記）
Device description: デバイスのディスクリプションを入力（Web UI上の表記）
Device key passphrase: Coreと共通のキーフレーズを入力
```

© 2019 Juniper Networks

Juniper Business Use Only

仮想サーバー設定手順(OVFファイル)

Wizard終了後、以下の設定を行います

・タイムゾーンの設定

```
Hostname-Core# server
Hostname-Core(server)# set timezone Asia/Tokyo
Current time zone is: JST (UTC+09:00)
```

・NTPサーバーの設定

```
Hostname-Core# server
Hostname-Core(server)# set ntpserver
Change the ntp server settings? (Yes/No)? yes
Enter the new ntp server name: xxxx.xxxx.xxxx.xxxx
```

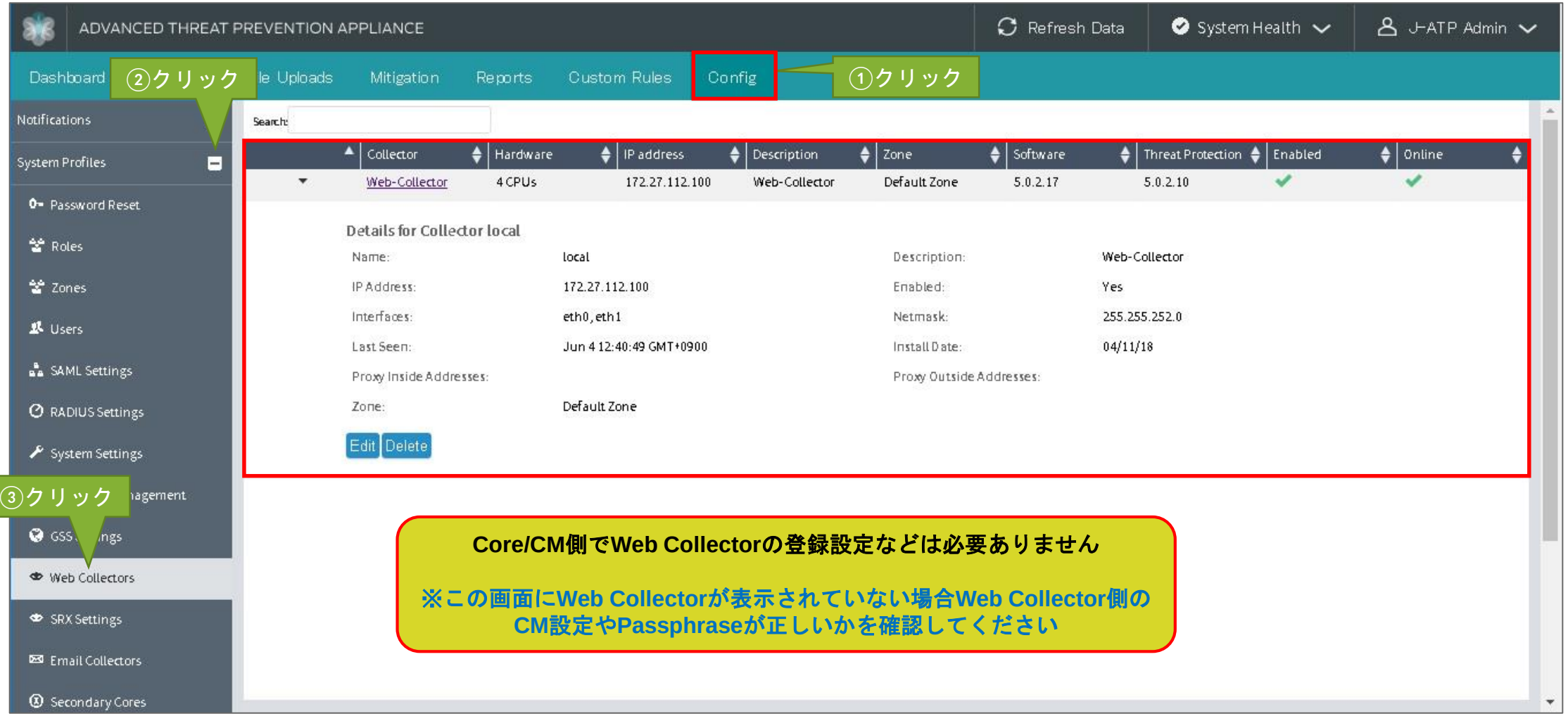
設定完了後、Core/CMのWeb UIへアクセスして
Web Collectorの接続確認を行います。
（Web Collector動作確認手順を参照）

© 2019 Juniper Networks

Juniper Business Use Only

Web Collector
動作確認手順

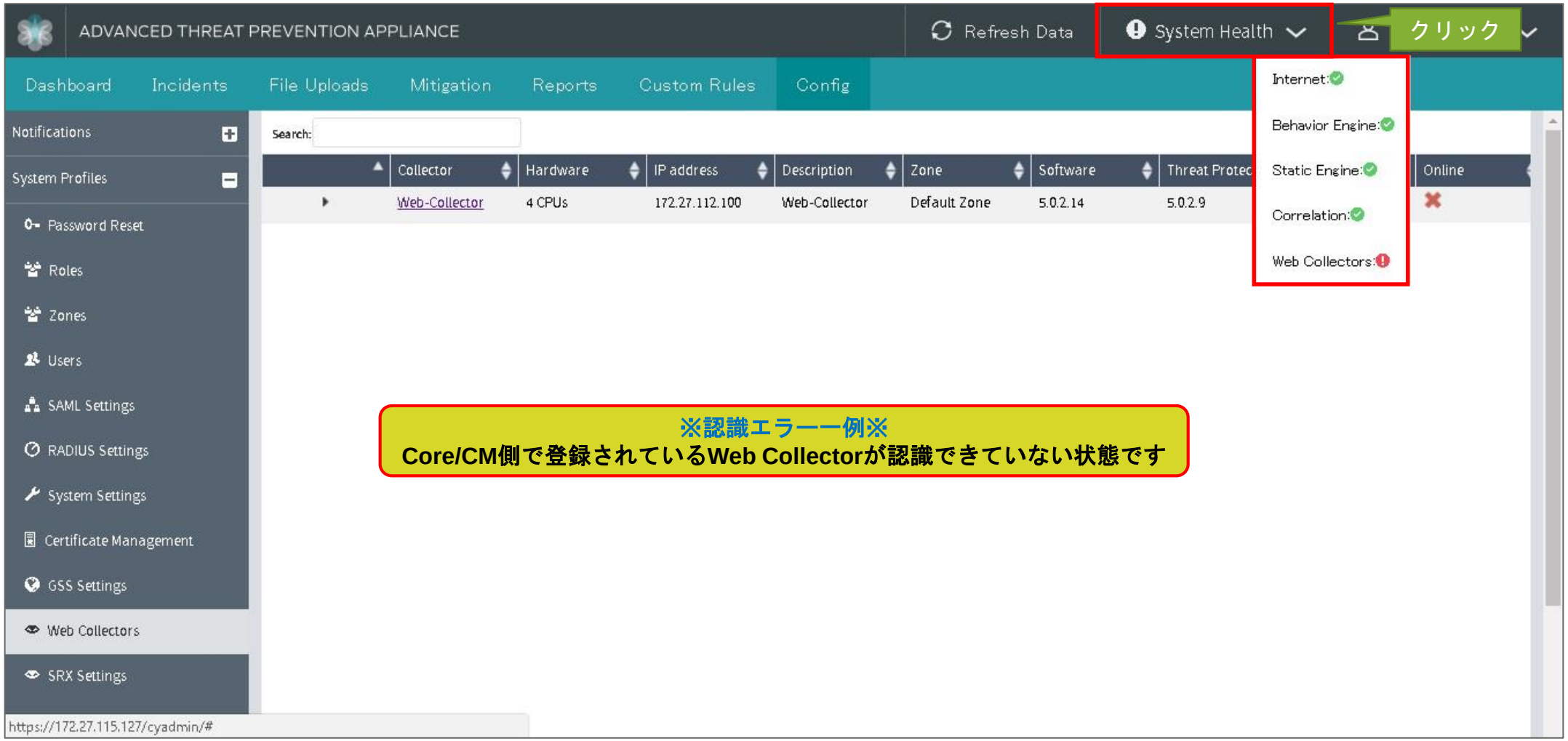
WEB COLLECTOR動作確認手順



© 2019 Juniper Networks

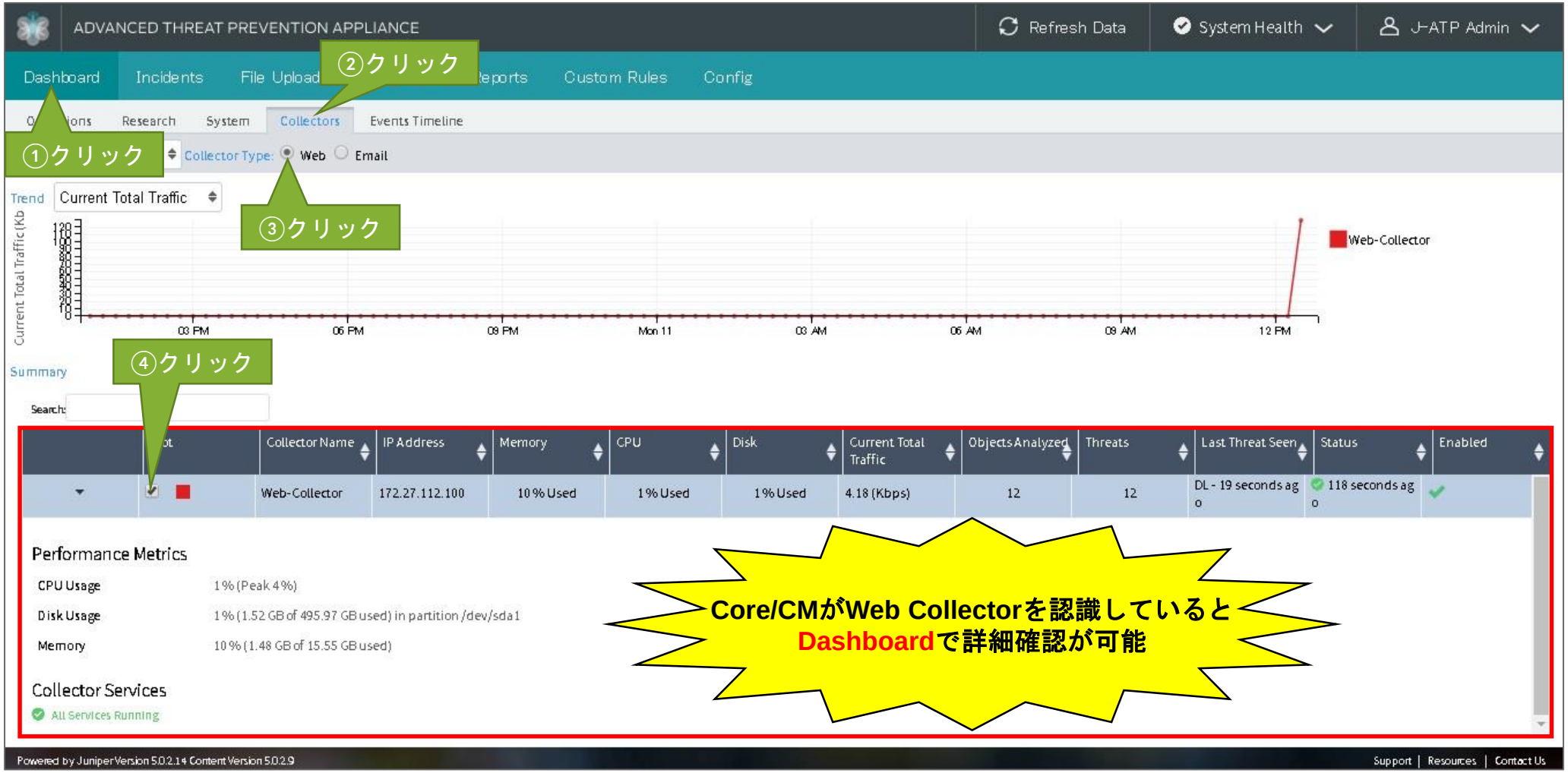
Juniper Business Use Only

WEB COLLECTOR動作確認手順



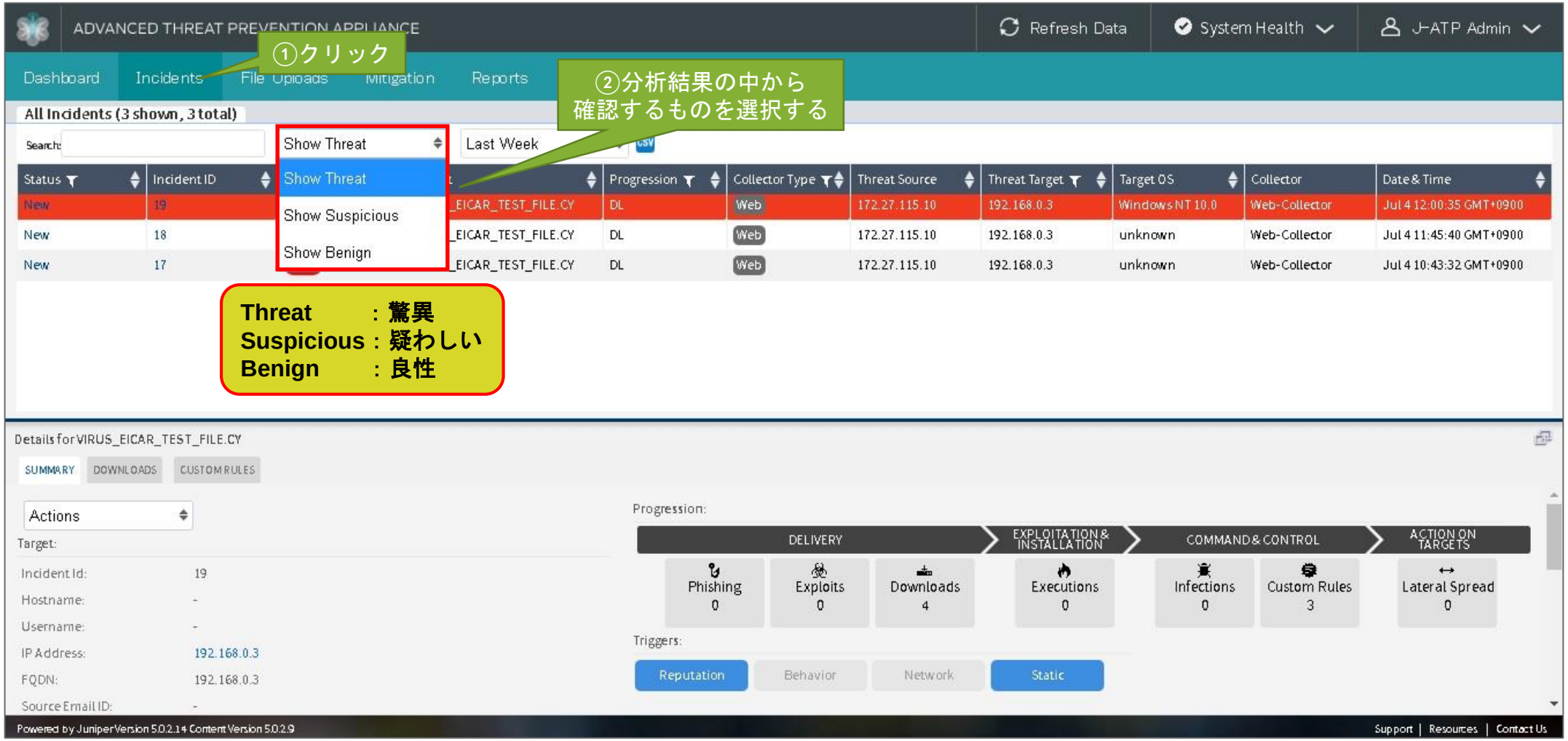
© 2019 Juniper Networks

WEB COLLECTOR動作確認手順



© 2019 Juniper Networks

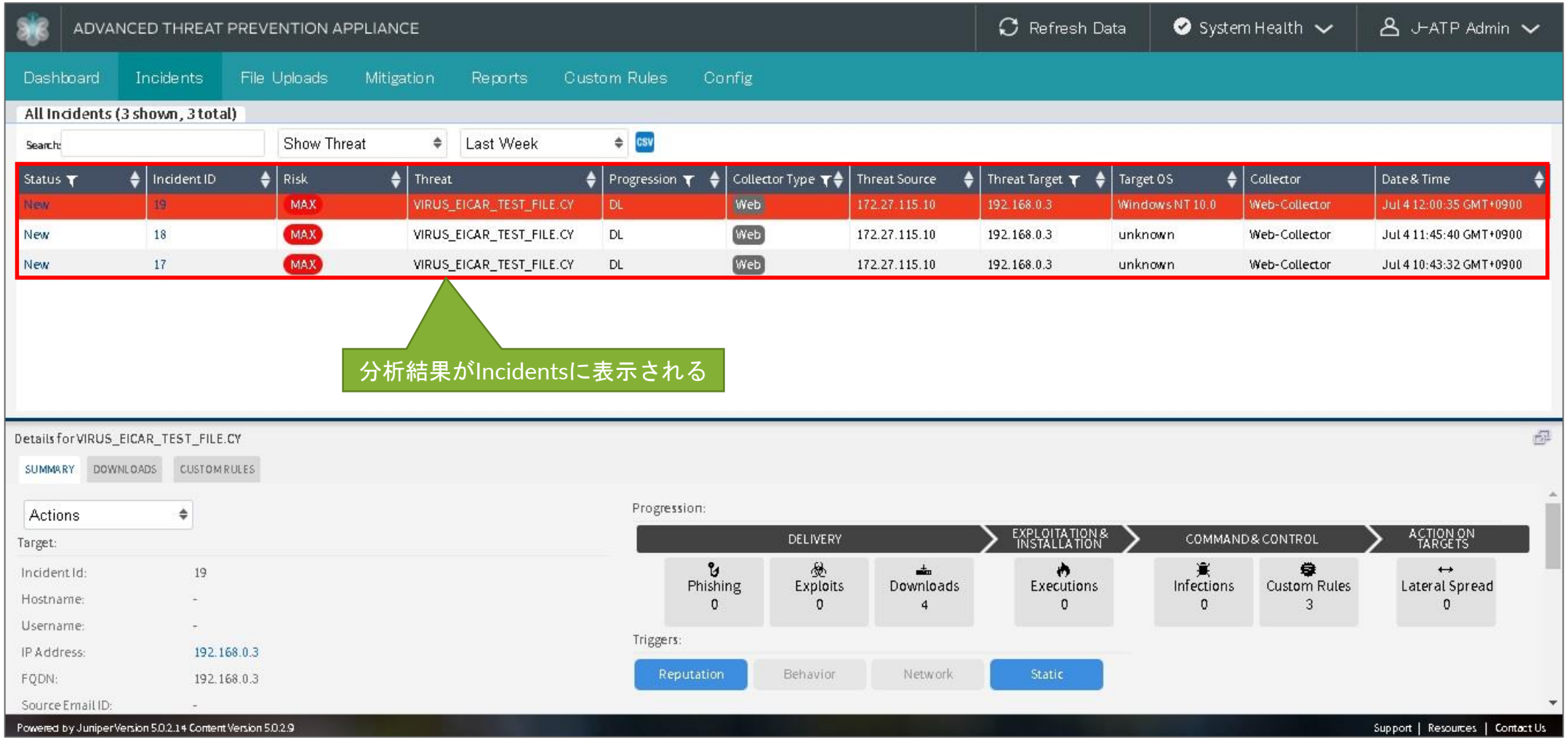
WEB COLLECTOR動作確認手順



© 2019 Juniper Networks

Juniper Business Use Only

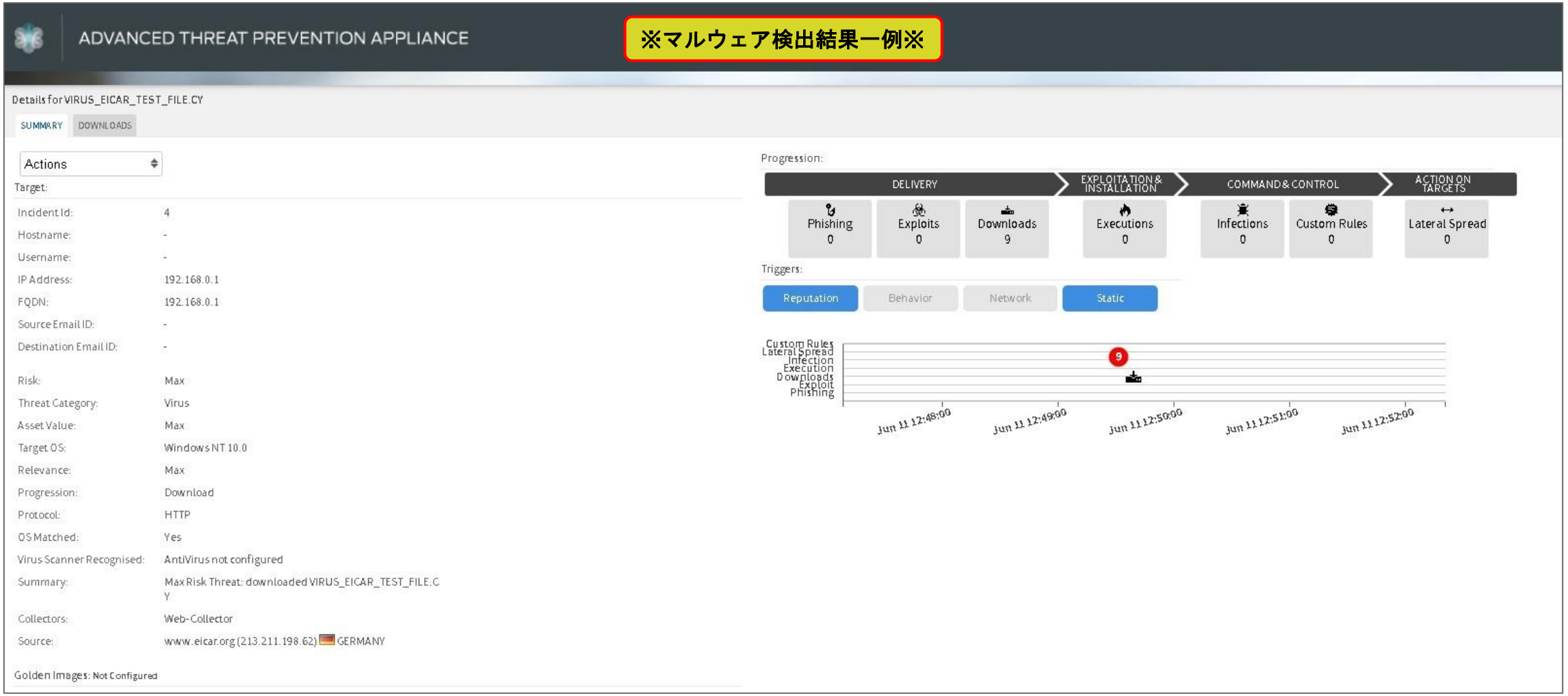
WEB COLLECTOR動作確認手順



© 2019 Juniper Networks

Juniper Business Use Only

WEB COLLECTOR動作確認手順



© 2019 Juniper Networks

Juniper Business Use Only

Web Collector
コマンド一例

WEB COLLECTORコマンド一例

CLI画面で設定の確認・変更を行う際は、各モードに入る必要があります

`Collector`	**Collector**の設定変更・確認 （Honeypotの設定、Traffic-filterの設定など）
`diagnosis`	Diagnosisの設定やステータス確認
`exit`	CLIセッションを終了
`help`	使用可能なSyntax一覧の表示
`history`	現在のセッションでのコマンド履歴の表示
`server`	Serverの設定変更・確認 （UUIDの確認、Pingの送信、サーバー設定の変更、サーバーの再起動など）
`wizard`	Wizardを起動して再設定

© 2019 Juniper Networks

Juniper Business Use Only

WEB COLLECTORコマンド一例

・インターフェース情報の確認

```
Web-collector# server
Web-collector(server)# show interface
 IP Address: 172.27.112.100 Mask: 255.255.252.0 MTU: 1500
  MAC Address: 00:50:56:b4:72:2c Speed: 10000Mb/s Duplex: Full
  Auto-negotiation: No Medium: Copper
  RX packets: 22746 Bytes: 3295924 Errors: 0 Overruns: 0
  TX packets: 2464 Bytes: 440321 Errors: 0 Overruns: 0
  Traffic rate for the last 5 seconds/1 minute/5 minutes
    RX bits/sec:    32640/38184/33528
    RX packets/sec: 28/30/28
    TX bits/sec:    3024/4528/4088
    TX packets/sec: 2/2/2

Interface: monitoring (eth1) Enabled: Yes Link: Yes
  IP Address: unknown Mask: unknown MTU: 1500
  MAC Address: 00:50:56:b4:94:e9 Speed: 10000Mb/s Duplex: Full
  Auto-negotiation: No Medium: Copper
  RX packets: 6 Bytes: 543 Errors: 0 Overruns: 0
  TX packets: 8 Bytes: 648 Errors: 0 Overruns: 0
  Traffic rate for the last 5 seconds/1 minute/5 minutes
    RX bits/sec:    0/0/0
    RX packets/sec: 0/0/0
    TX bits/sec:    0/0/0
    TX packets/sec: 0/0/0
```

© 2019 Juniper Networks

Juniper Business Use Only

WEB COLLECTORコマンド一例

・IPアドレスの個別設定

```
Web-collector# server
Web-collector(server)# set ip interface
Use DHCP to obtain an IP address for management (eth0) interface (Yes/No)? yes / no
Enter IP address for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
Enter netmask for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
Enter gateway IP Address for the management (eth0) interface: xxxx.xxxx.xxxx.xxxx
```

・CMの指定

```
Web-collector# server
Web-collector(server)# set cm xxxx.xxxx.xxxx.xxxx
```

・CLIログインパスワードの変更

```
Web-collector# server
Web-collector(server)# set password
Enter the current password of CLI admin: 現在のパスワード
Enter the new password of CLI admin: 新しいパスワード
Retype the new password of CLI admin: 新しいパスワードを再入力
```

・タイムゾーンの設定

```
Web-collector# server
Web-collector(server)# set timezone Asia/Tokyo
```

© 2019 Juniper Networks

Juniper Business Use Only

WEB COLLECTORコマンド一例

・NTPサーバーの設定
```
Web-collector# server
Web-collector(server)# set ntpserver
Change the ntp server settings? (Yes/No)? yes
Enter the new ntp server name: xxxx.xxxx.xxxx.xxxx
```

・Pingの送信
```
Web-collector# server
Web-collector(server)# ping xxxx.xxxx.xxxx.xxxx
```

・サーバーのシャットダウン
```
Web-collector# server
Web-collector(server)# shutdown
```

・セットアップチェック
```
Web-collector# diagnosis
Web-collector(diagnosis)# setupcheck all / report / basic / analysis
```

・パケットキャプチャー
```
Web-collector# diagnosis
Web-collector(server)# capture-start
```

・キャプチーファイルのコピー
```
Web-Collector# diagnosis
Web-Collector(diagnosis)# copy capture user@hostname:path
```

© 2019 Juniper Networks

Juniper Business Use Only

THANK YOU
JUNIPER NETWORKS
Engineering
Simplicity