

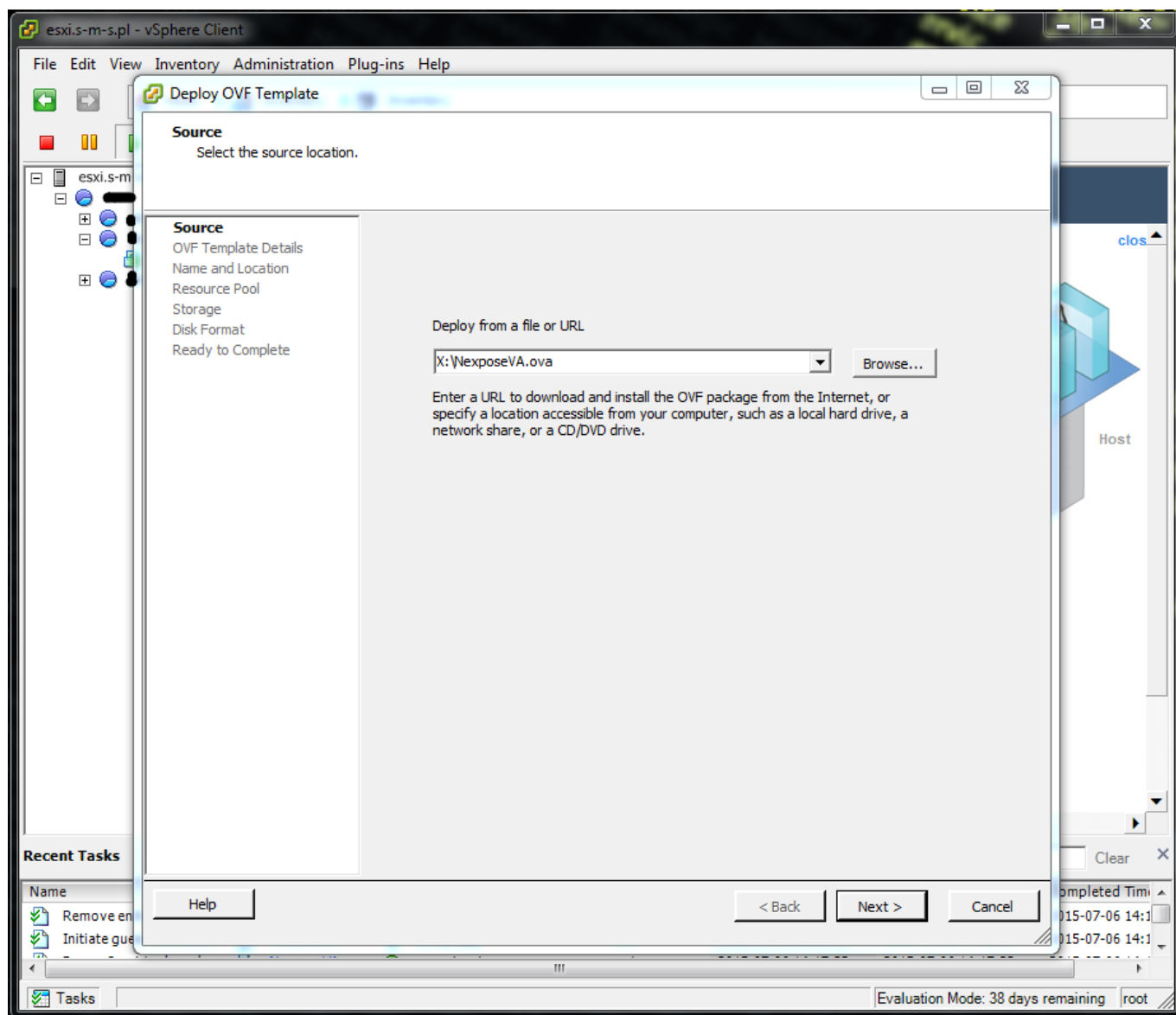


Po krótkiej przerwie powracamy do pisania postów i z tej okazji postanowiłem wypuścić kolejny - drugi - odcinek serii o zarządzaniu podatnościami. Dziś postaram się przekazać Wam jak poprawnie skonfigurować skaner podatności Nexpose.

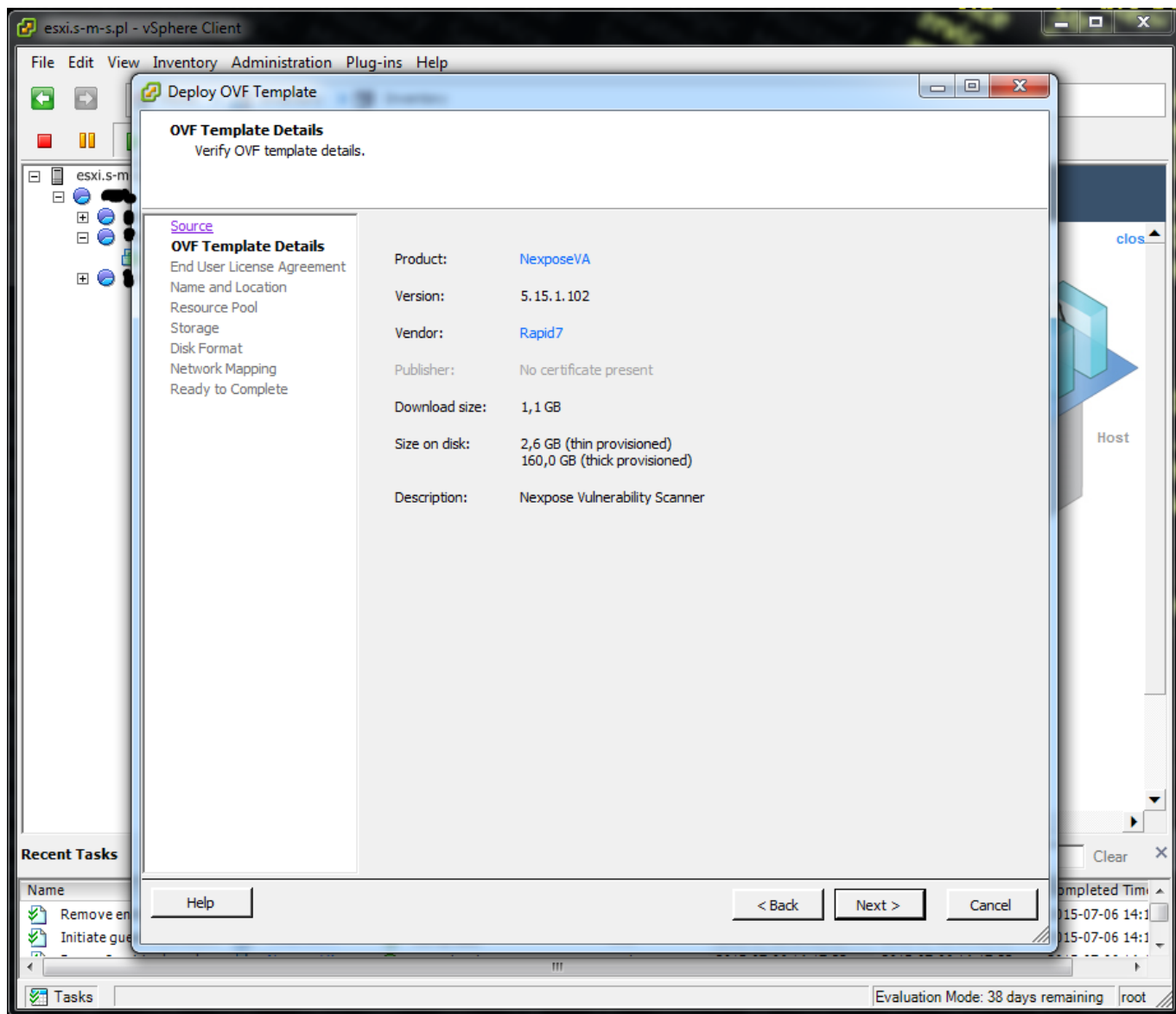
Przedstawię dzisiaj instalację i konfigurację za pomocą pliku .ovf, czyli wirtualnej maszyny przygotowanej do instalacji na serwerze wirtualizacji, oraz manualnej instalacji Nexpose na wcześniej przygotowanym systemie operacyjnym. Artykuł zawiera dużą ilość screenów, które mają charakter poglądowy i w większości nie wymagają komentarza.

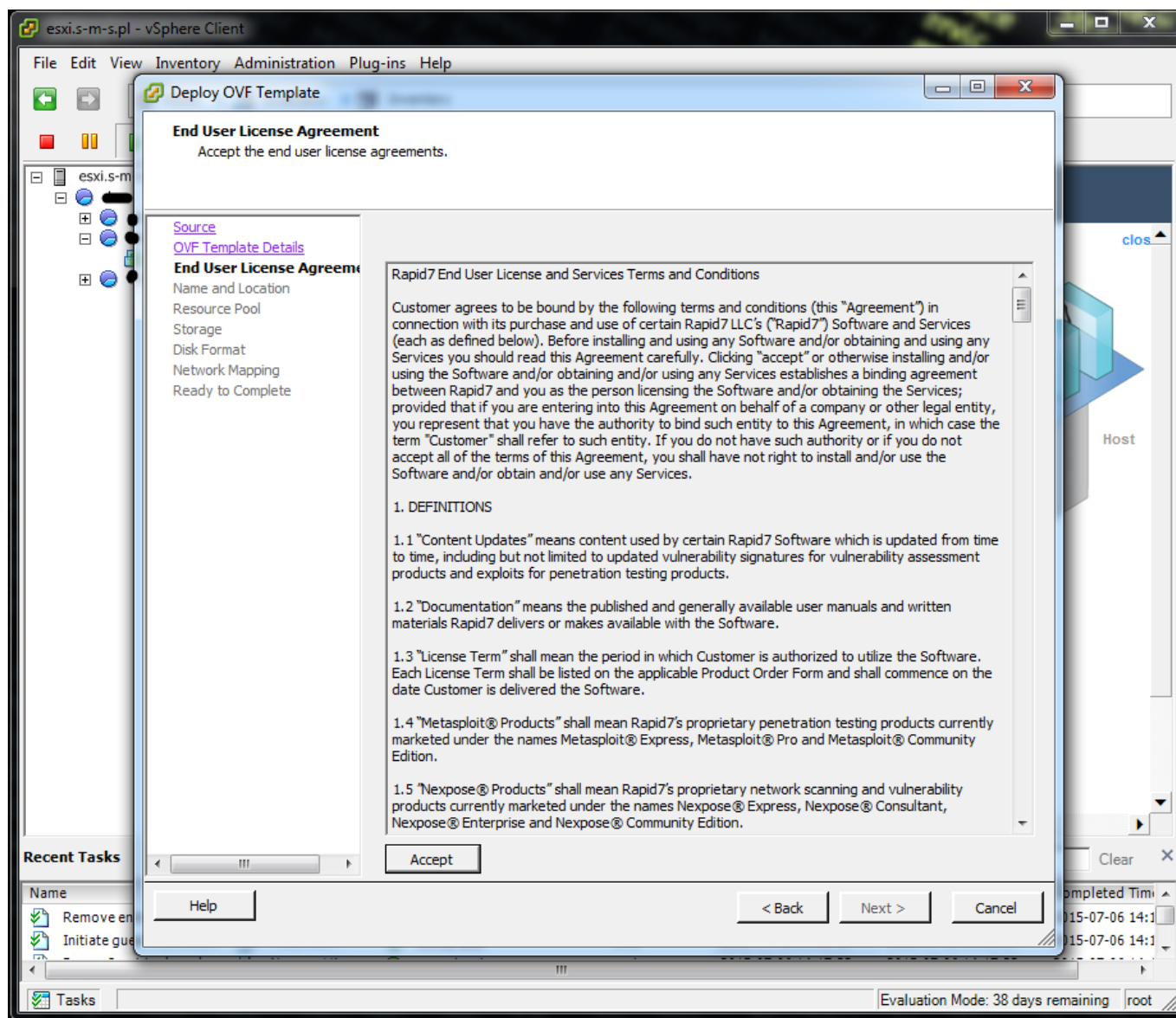
Instalacja z gotowego obrazu .ova.

Do wirtualizacji użyję serwera ESXi w wersji 5.5.

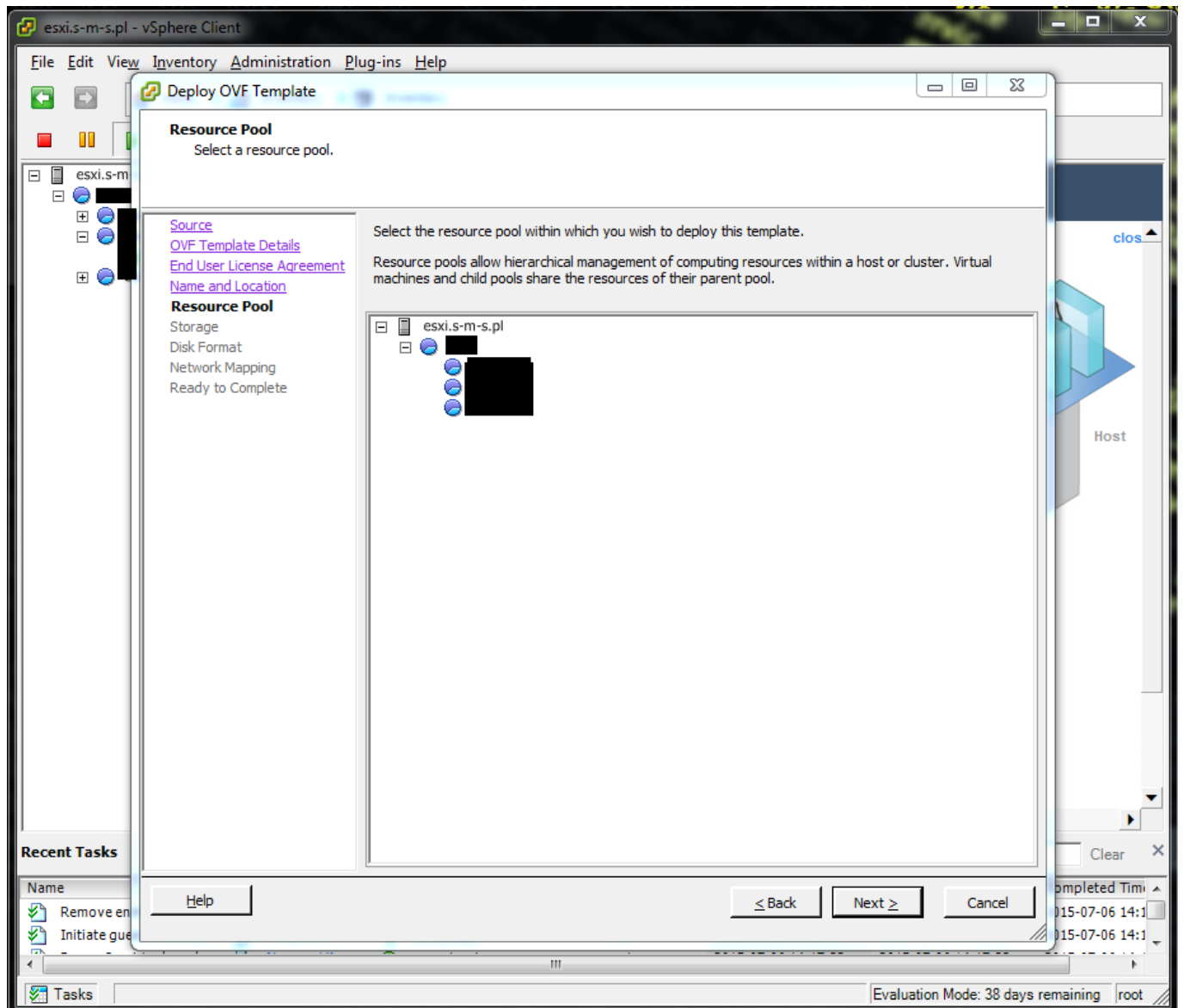


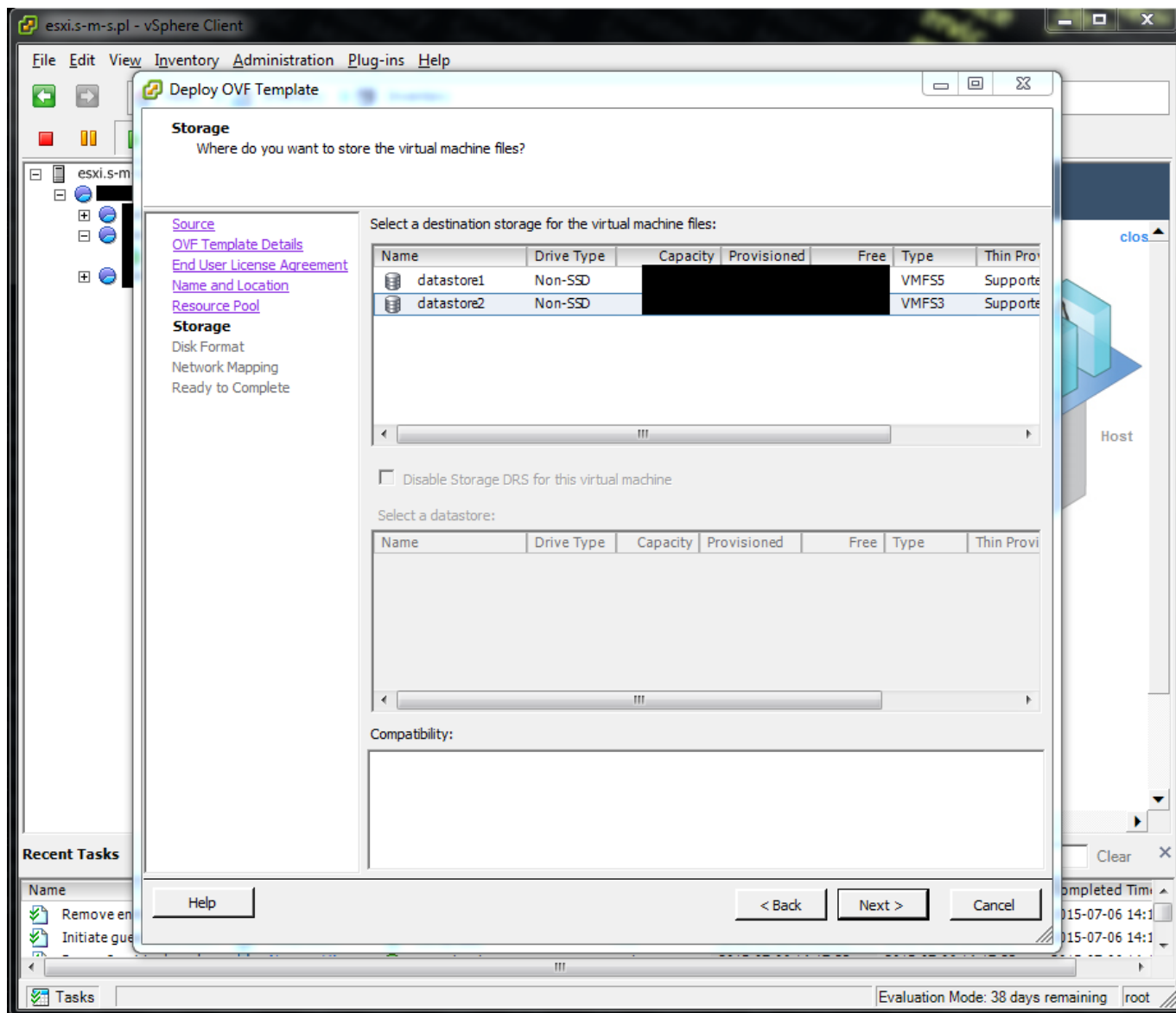
Pierwszym co musimy zrobić to wczytać obraz maszyny wirtualnej pobranej ze strony Rapid7.

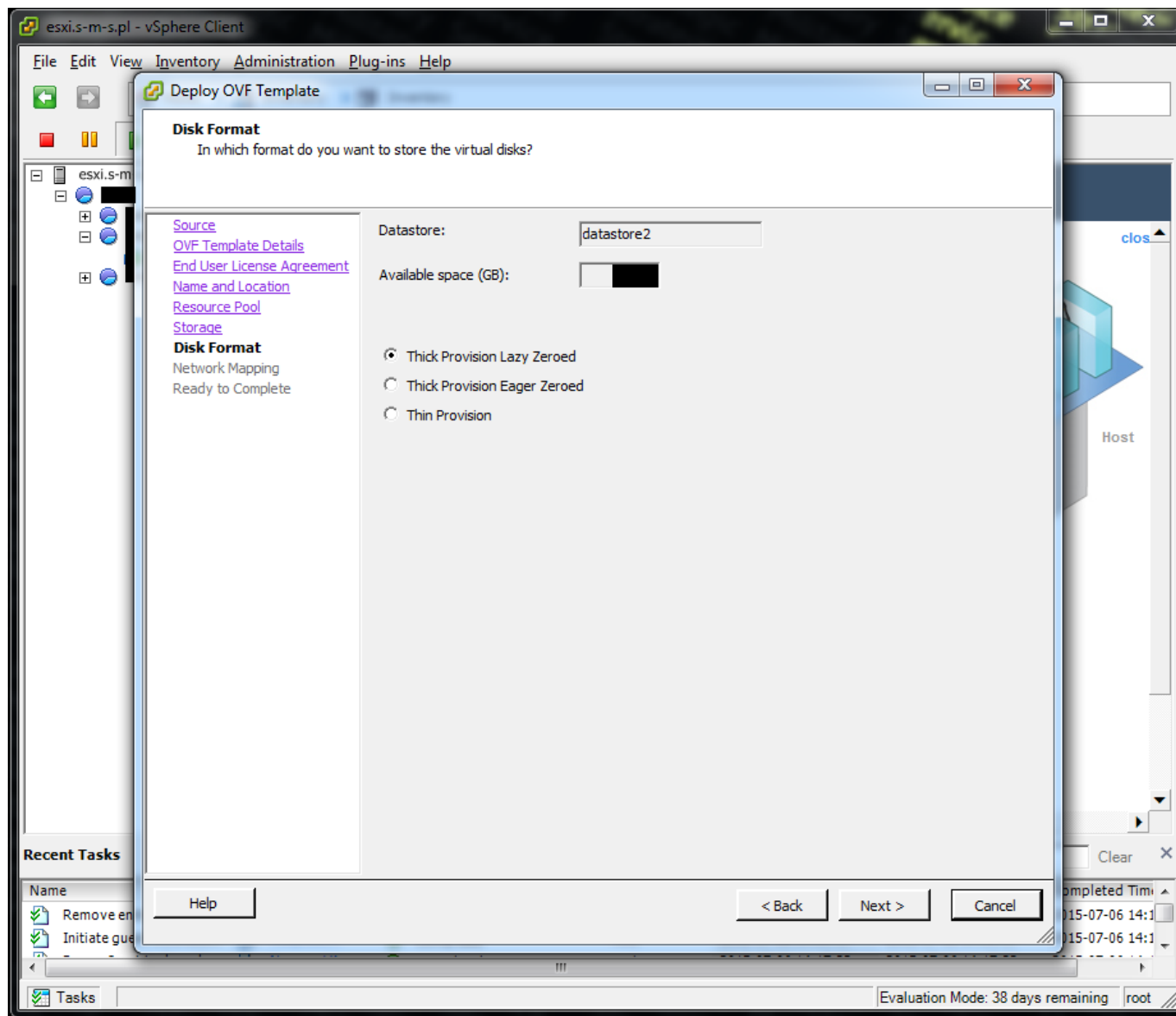


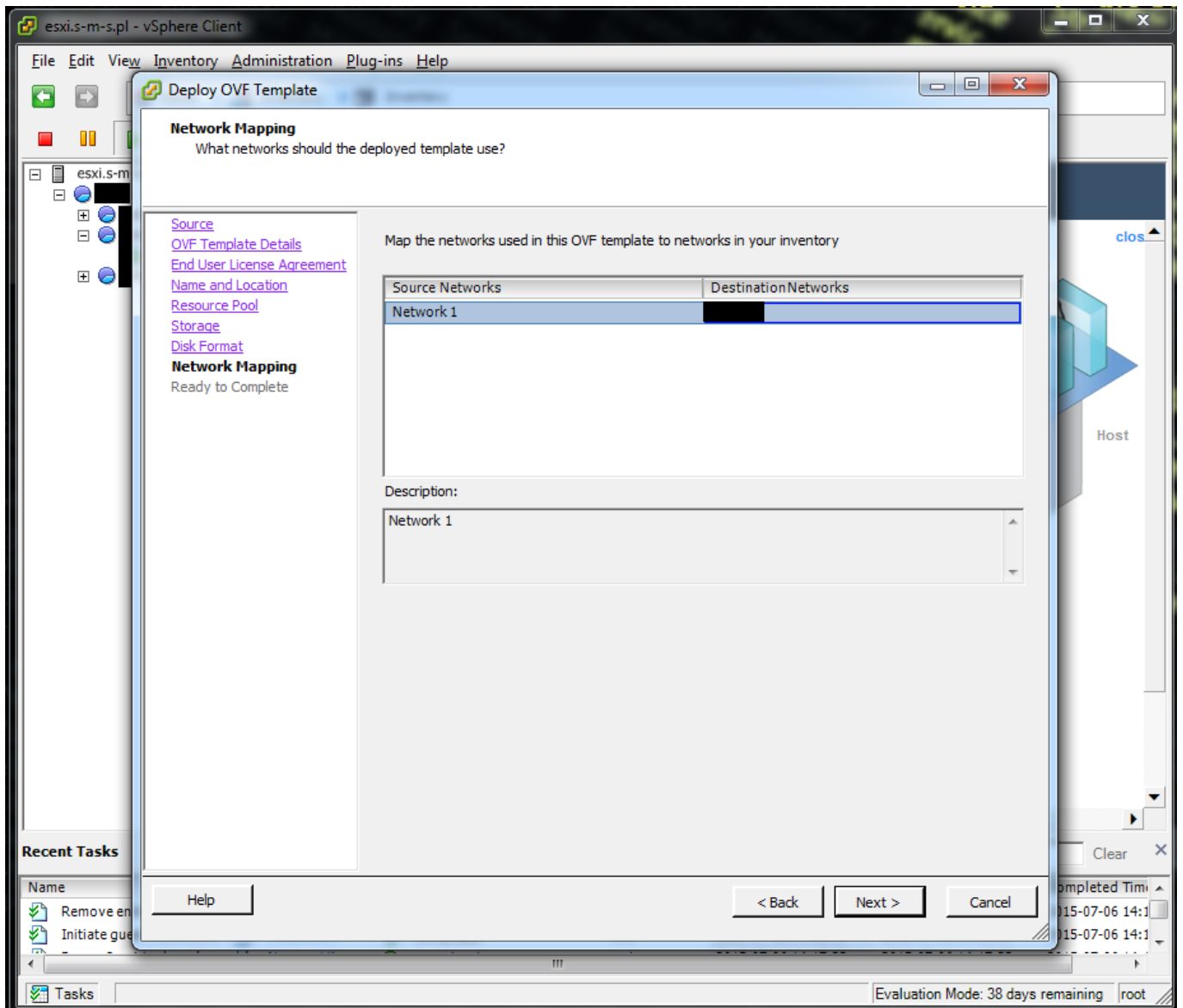


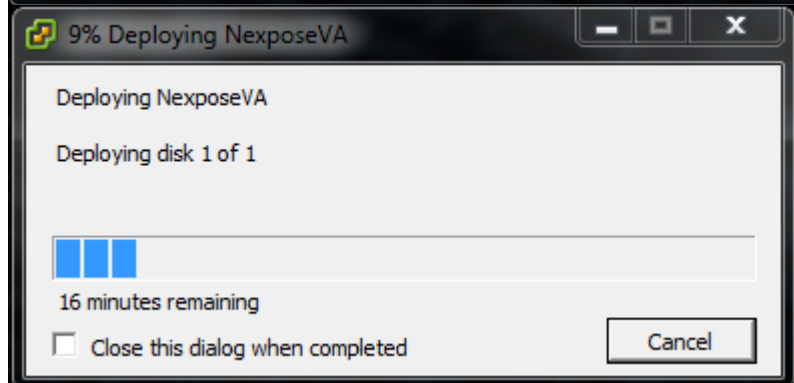
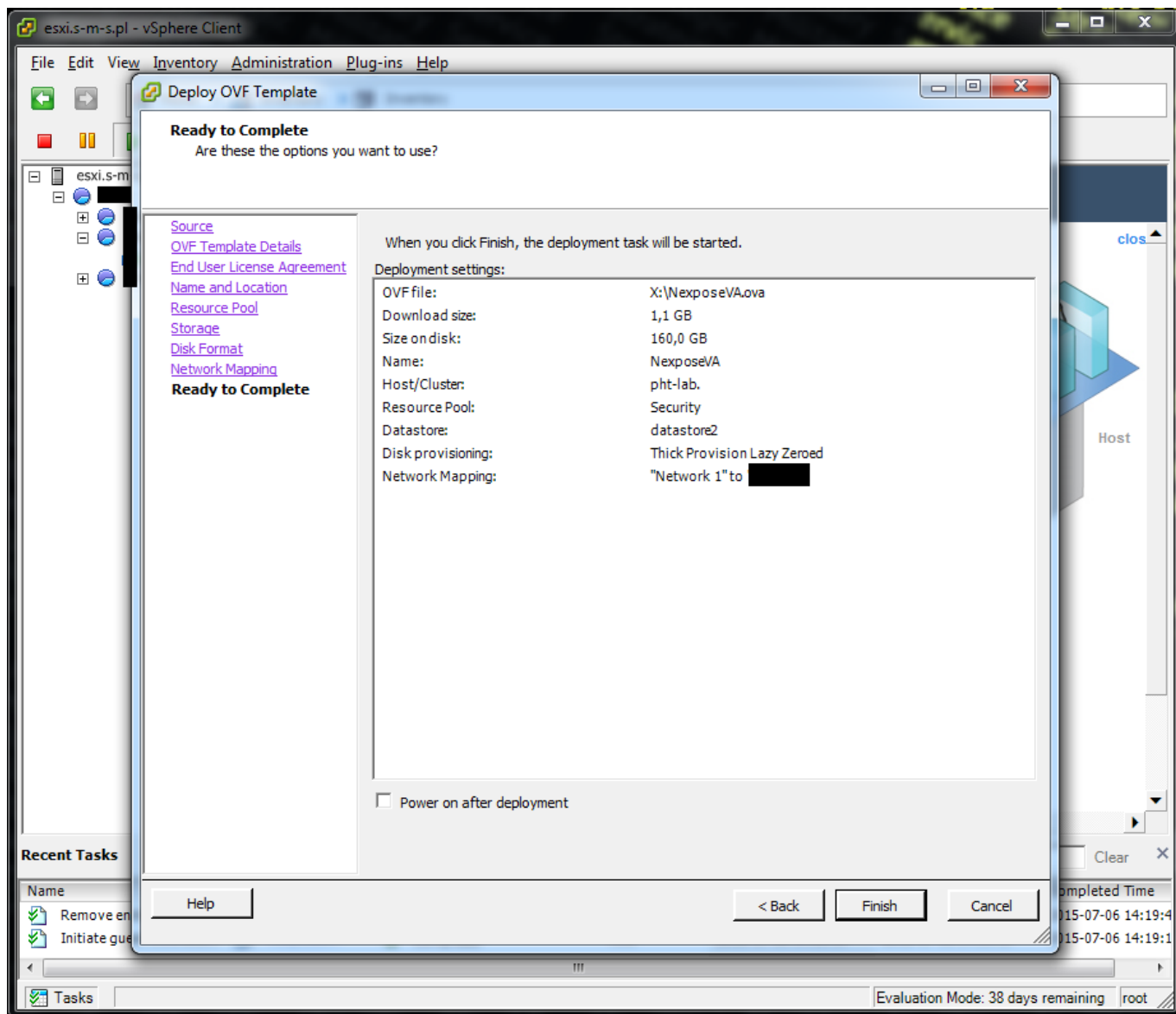
Zapoznajemy się z EULA i akceptujemy postanowienia licencji.

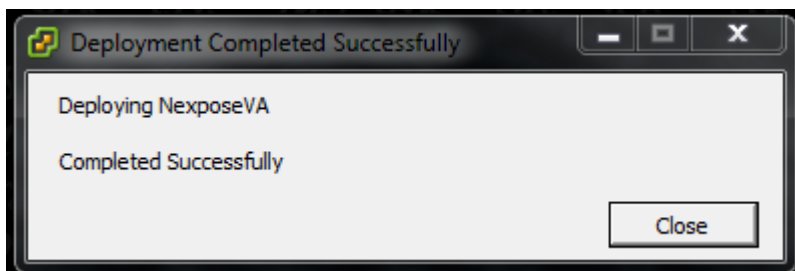












esxi.s-m-s.pl - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Inventory Inventory

esxi.s-m-s.pl

- NexposeVA

NexposeVA

Summary Resource Allocation Performance Events Console Permissions

General

Guest OS: Ubuntu Linux (64-bit)
 VM Version: 7
 CPU: 2 vCPU
 Memory: 5120 MB
 Memory Overhead: 191,59 MB
 VMware Tools: ⚠ Not running (Out-of-date)
 IP Addresses:
 DNS Name:
 State: Powered Off
 Host: pht-lab
 Active Tasks:
 vSphere HA Protection: ? N/A ?

Resources

Consumed Host CPU:
 Consumed Host Memory:
 Active Guest Memory:
 Provisioned Storage: Refresh Storage Usage **165,25 GB**
 Not-shared Storage: **160,00 GB**
 Used Storage: **160,00 GB**

Storage	Drive Type	Capacity
datastore2	Non-SSD	

Network Type

Network	Type
	Standard port group

Commands

▶ Power On
🔧 Edit Settings

Annotations

Notes: Nexpose Vulnerability Scanner ✎ Edit

Recent Tasks Name, Target or Status contains: Clear

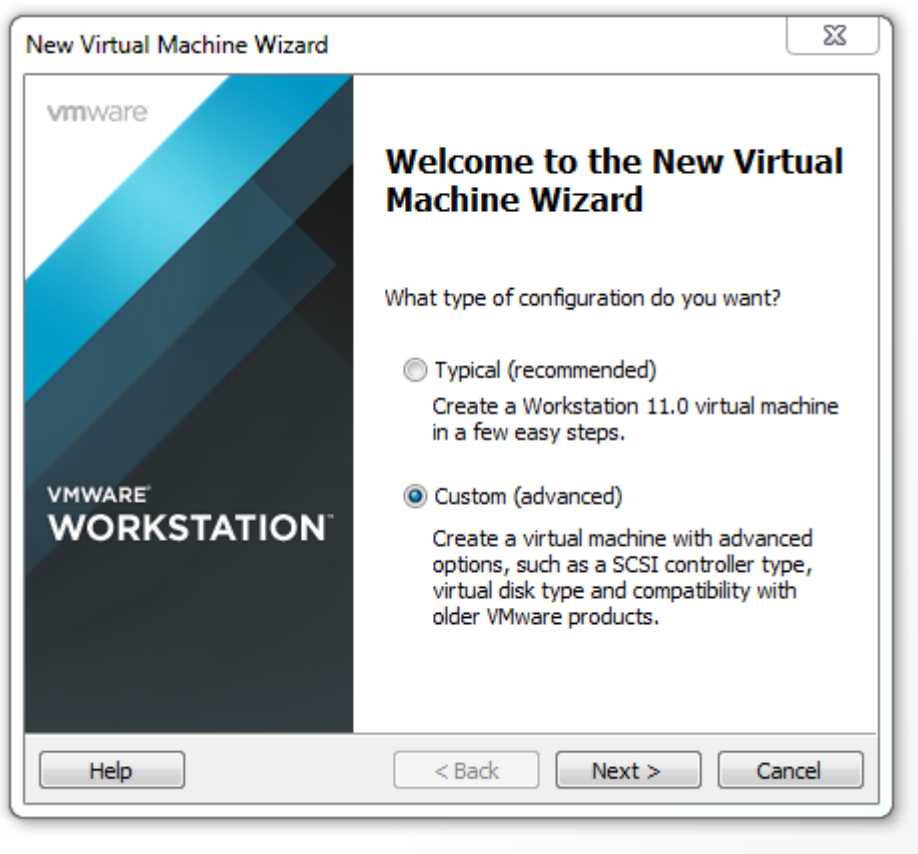
Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time

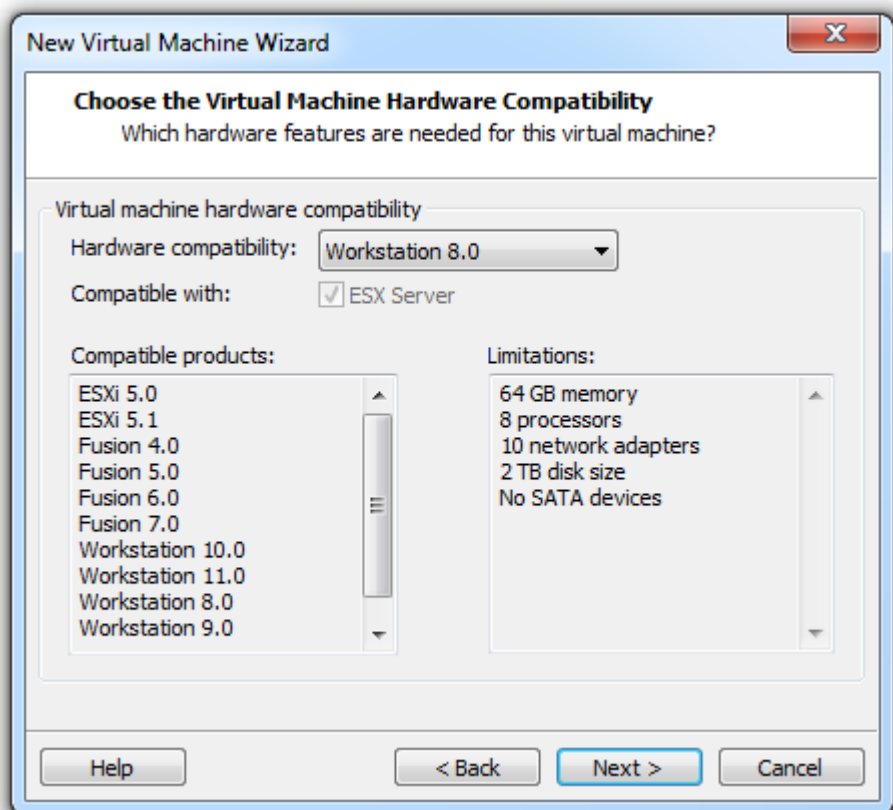
Tasks Evaluation Mode: 38 days remaining root

Instalacja manualna z pliku binarnego.

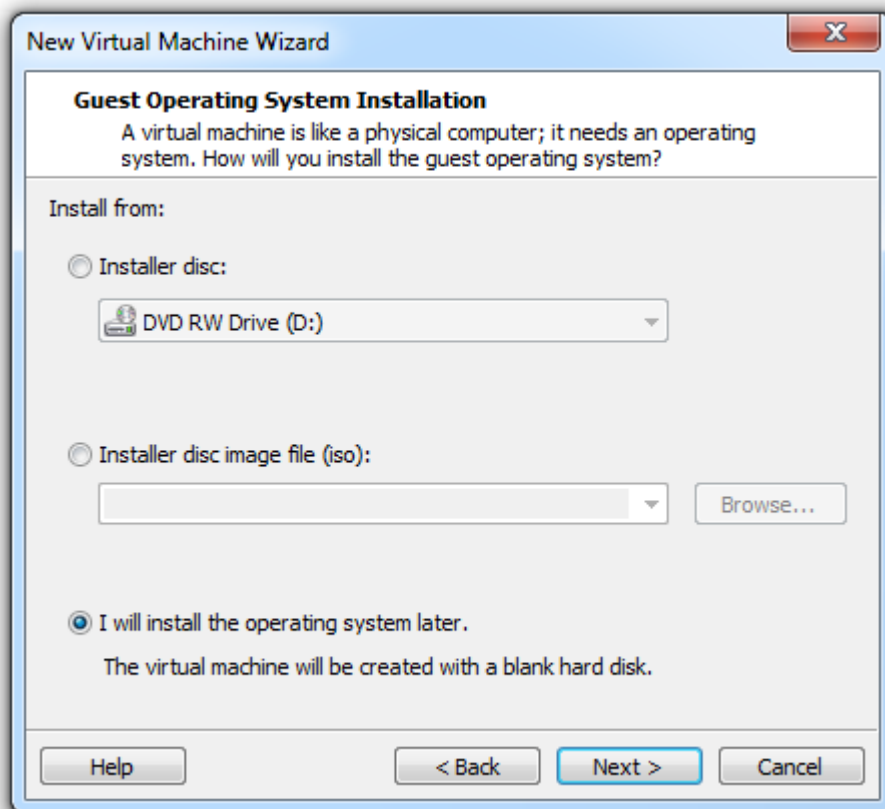
Przygotowanie wirtualnej maszyny.

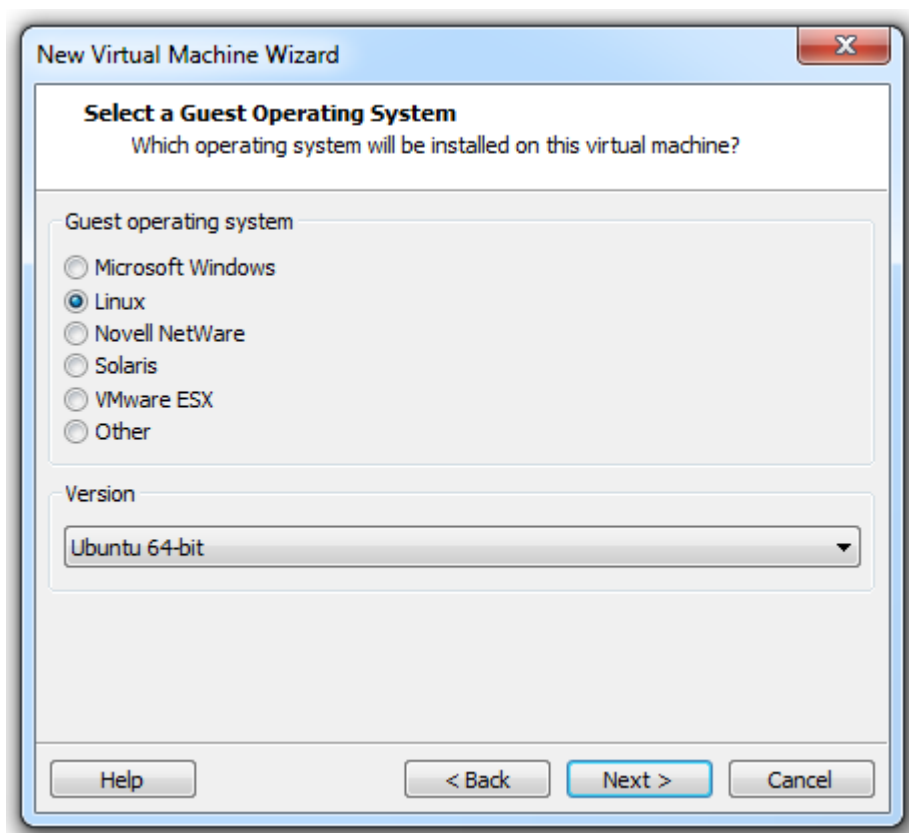
Alternatywą dla tego sposobu jest ręczna instalacja. Pierwszym co musimy zrobić to utworzenie nowej maszyny, lub wykorzystanie fizycznej maszyny i instalacja jednego z wspieranych systemów operacyjnych. Listę systemów wymieniliśmy [tutaj](#). Wybraliśmy Ubuntu w wersji 14.04. Poniżej procedura przygotowania maszyny w VMware Workstation. Zalecamy przy tworzeniu maszyny wybranie opcji „Custom”.

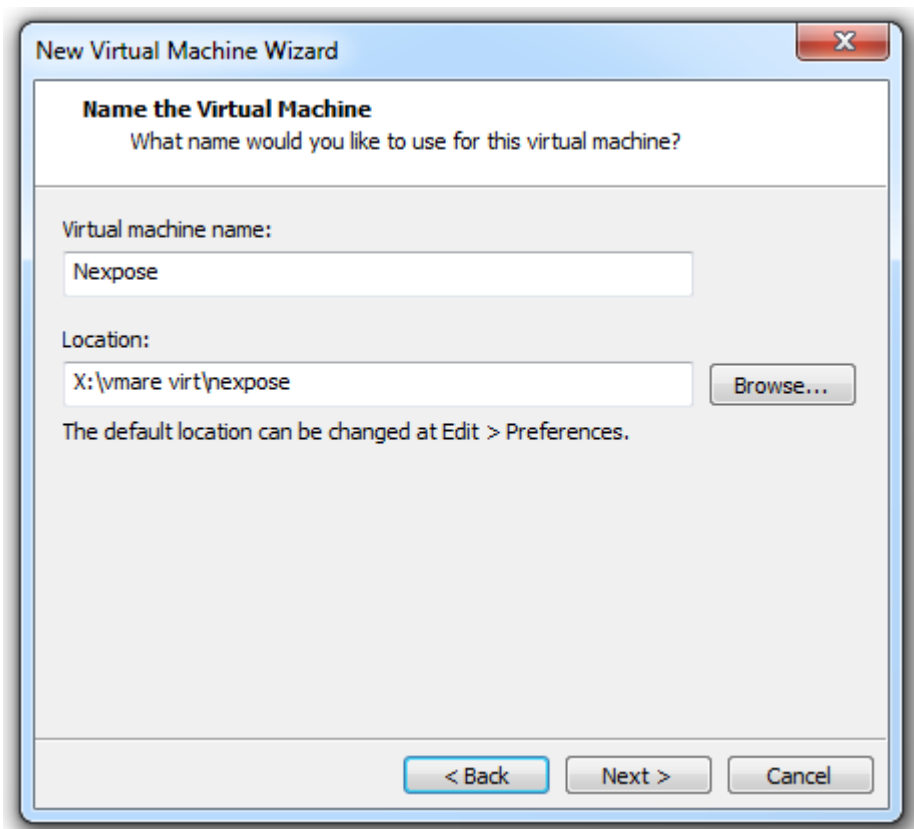




Wybieramy wersję Workstation 8.0, tak by przygotowany przez nas obraz mógł być wczytany do serwera wirtualizacji ESXi.







New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Nexpose

Location:
X:\vmare virt\nexpose

The default location can be changed at Edit > Preferences.

< Back Next > Cancel

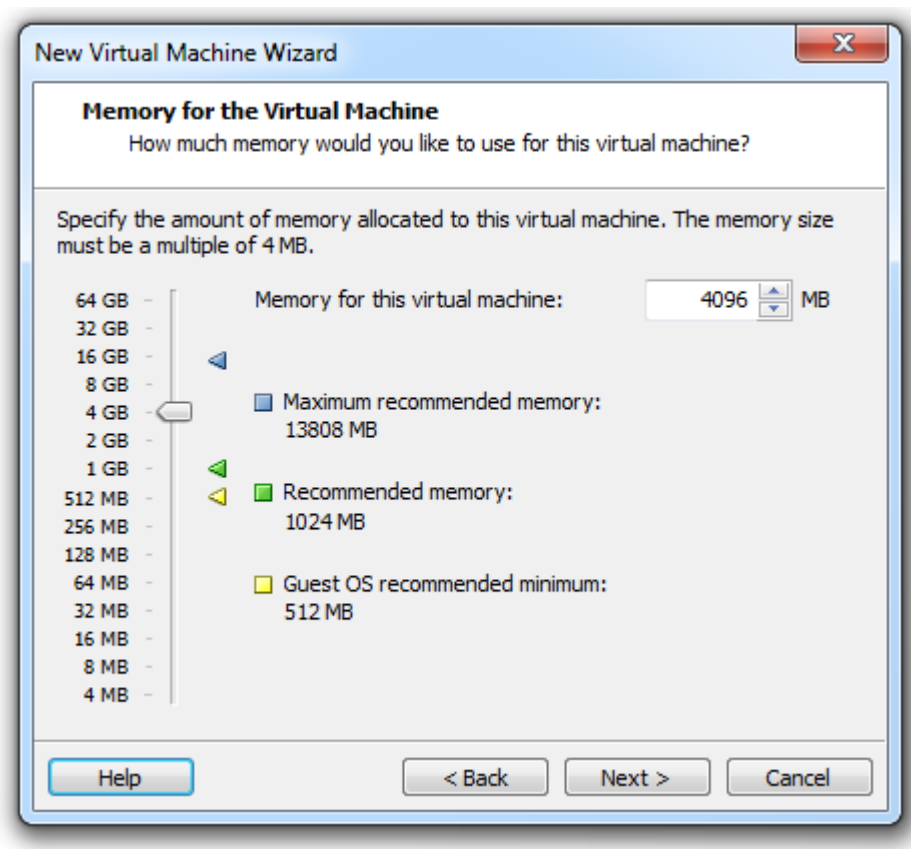
New Virtual Machine Wizard

Processor Configuration
Specify the number of processors for this virtual machine.

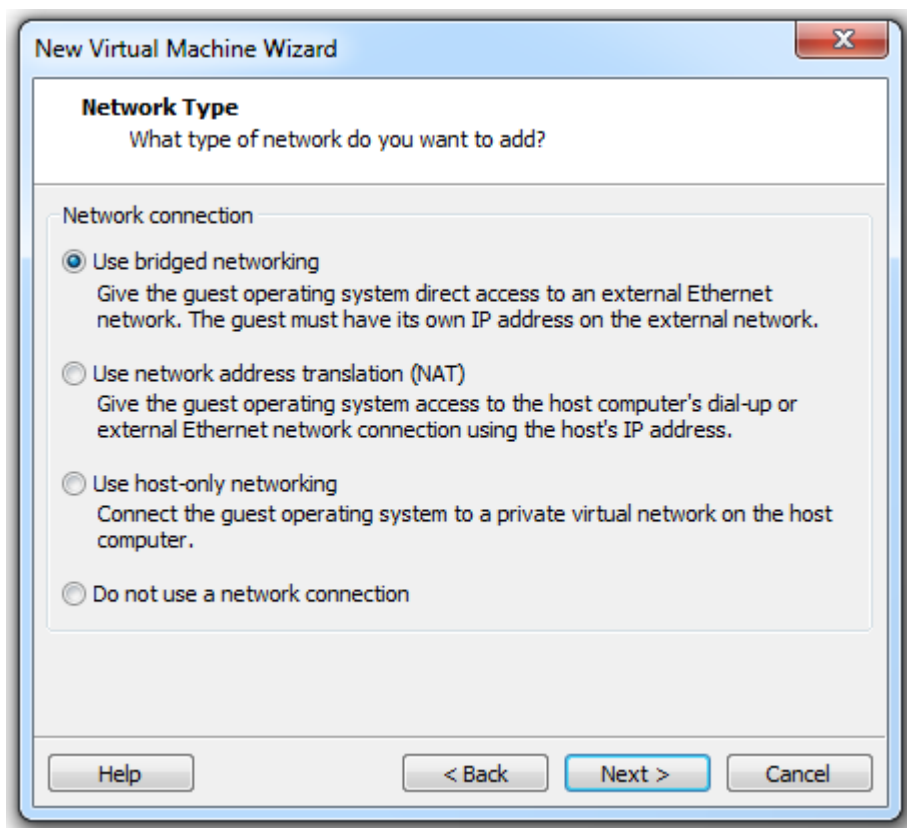
Processors

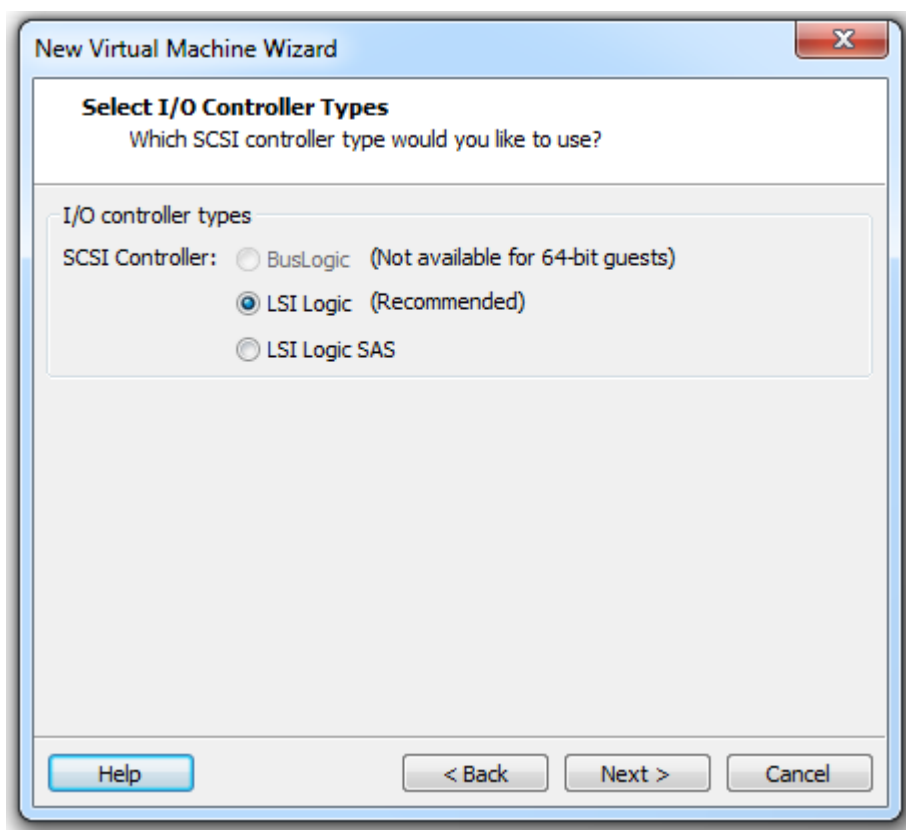
Number of processors:	2
Number of cores per processor:	4
Total processor cores:	8

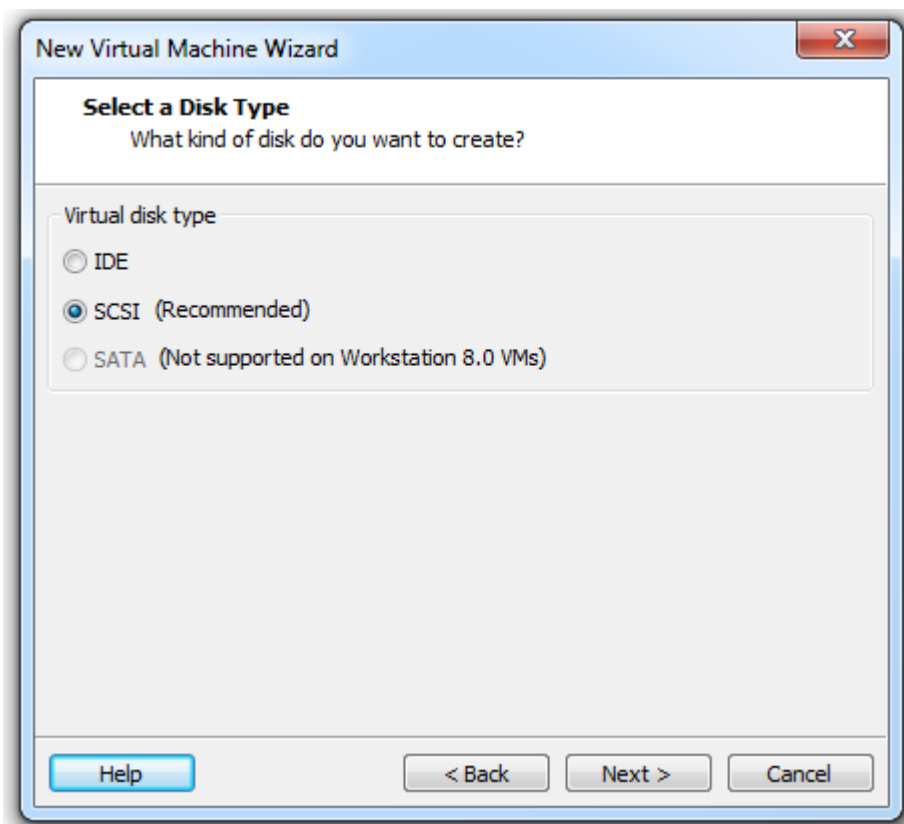
Help < Back Next > Cancel

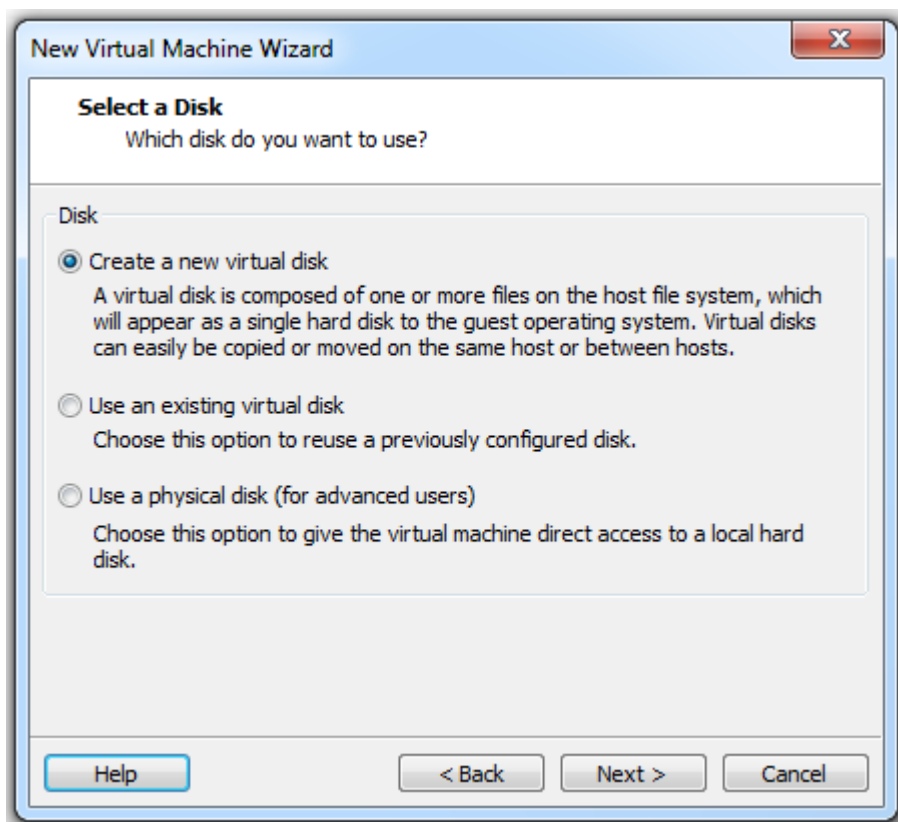


Zalecanym przez Rapid7 jest ustawienie 16 GB ramu dla nexpose, minimalnie zaś 8 GB. Spokojnie można ustawić 4 GB, skany będą się odbywać wolniej, ale do labu w zupełności wystarczy.

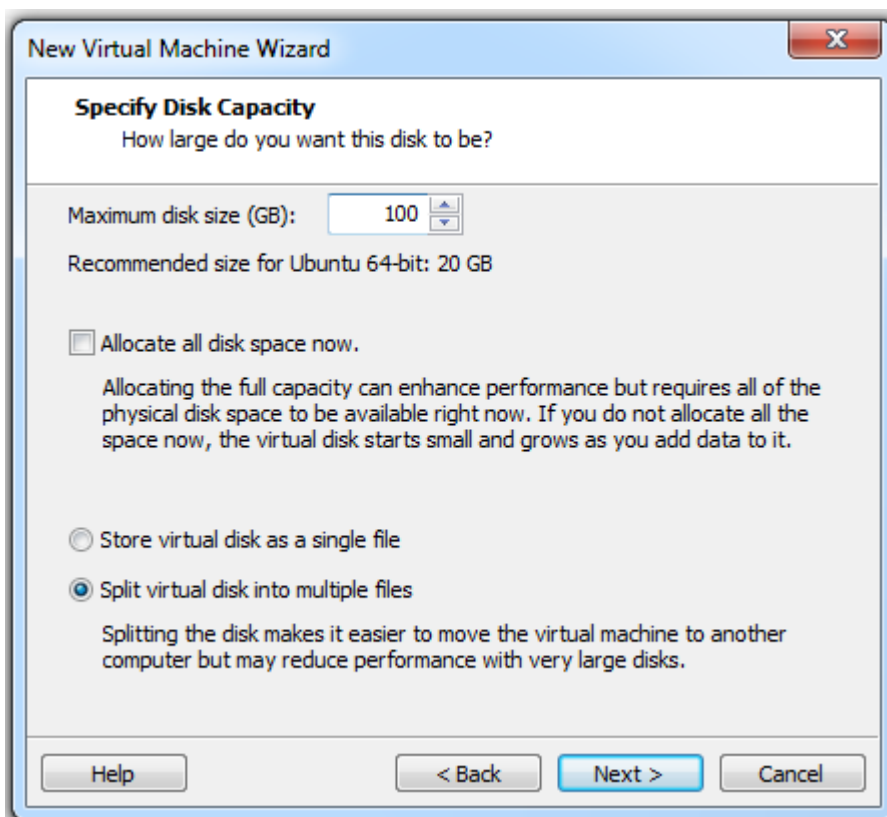




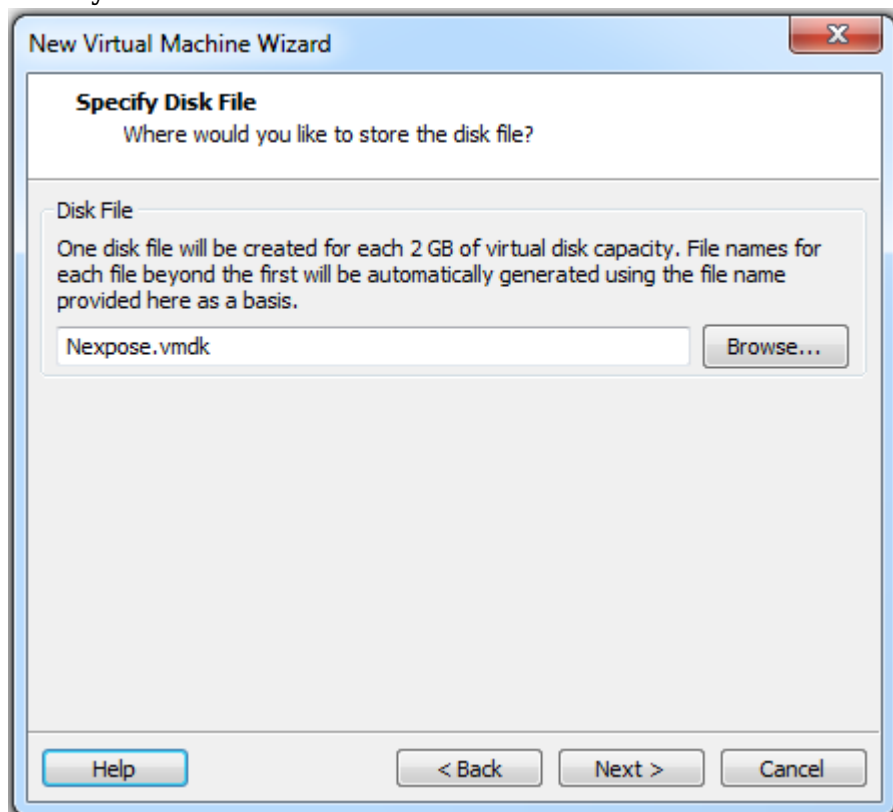


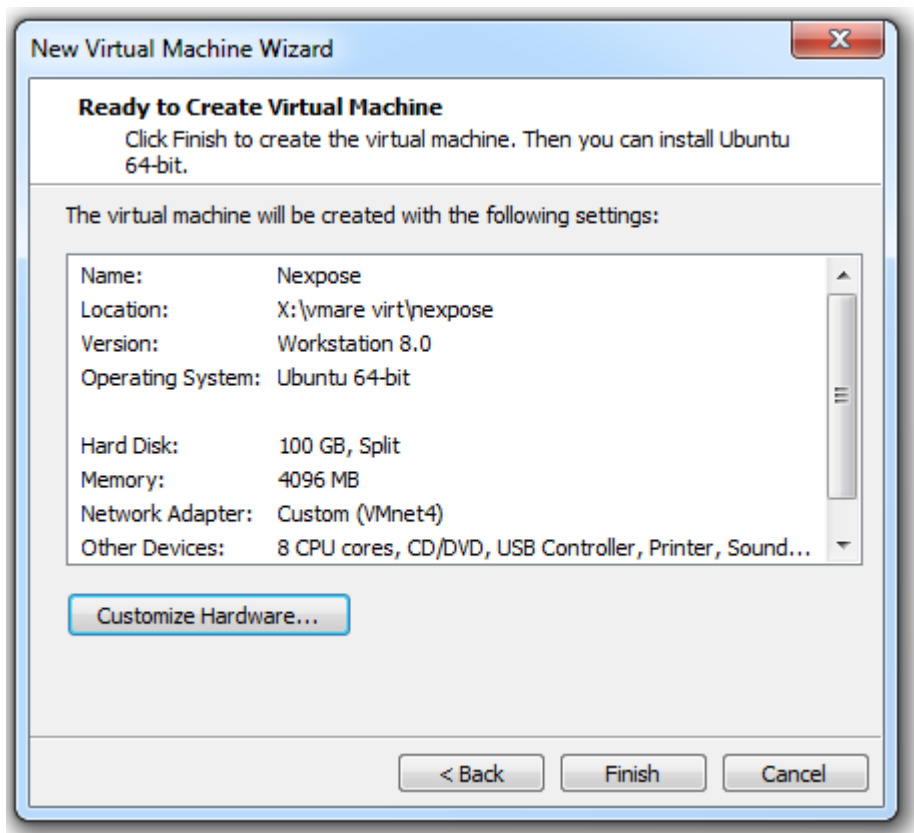


Jeżeli chodzi o przestrzeń dyskową, zalecany jest 80+ GB, my polecamy trzymanie się



zasady 100+ GB.







Nexpose

- ▶ Power on this virtual machine
- ▶ Edit virtual machine settings
- ▶ Upgrade this virtual machine

▼ **Devices**

Memory	4 GB
Processors	8
Hard Disk (SCSI)	100 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet4)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

▼ **Description**

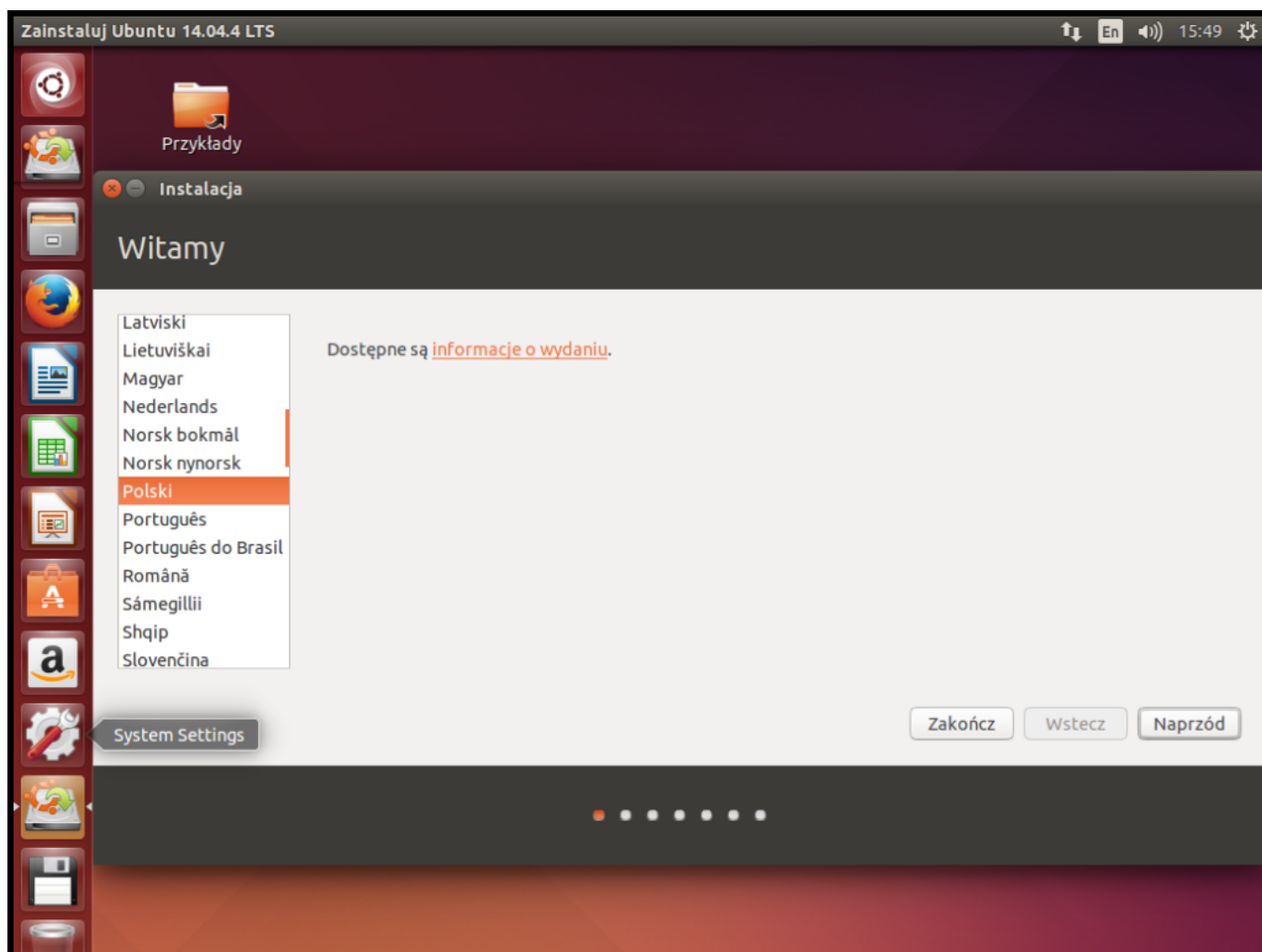
Type here to enter a description of this virtual machine.



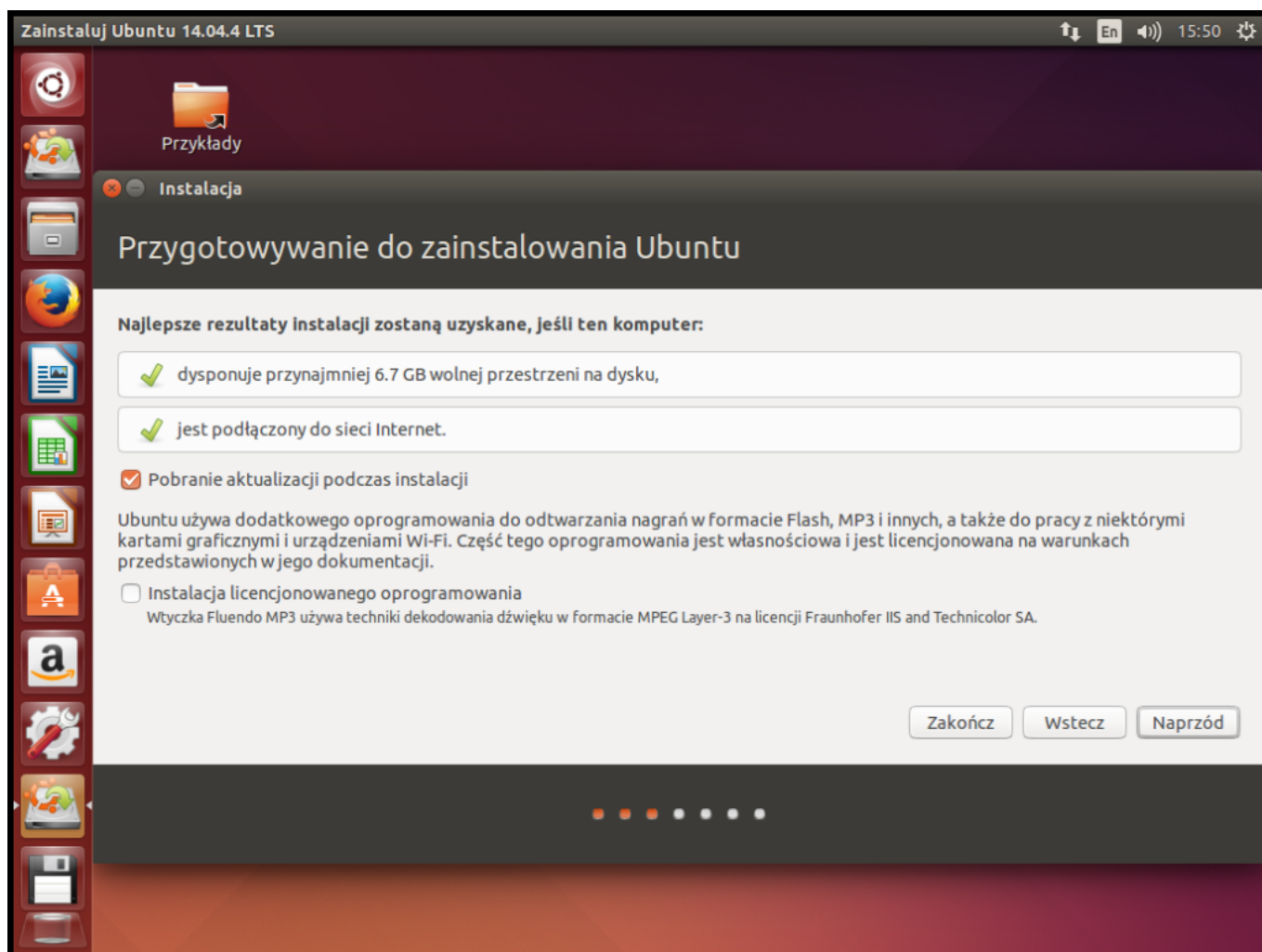
▼ **Virtual Machine Details**

State: Powered off
Configuration file: X:\vmare virt\nexpose\nexpose.vmx
Hardware compatibility: Workstation 8.0 virtual machine

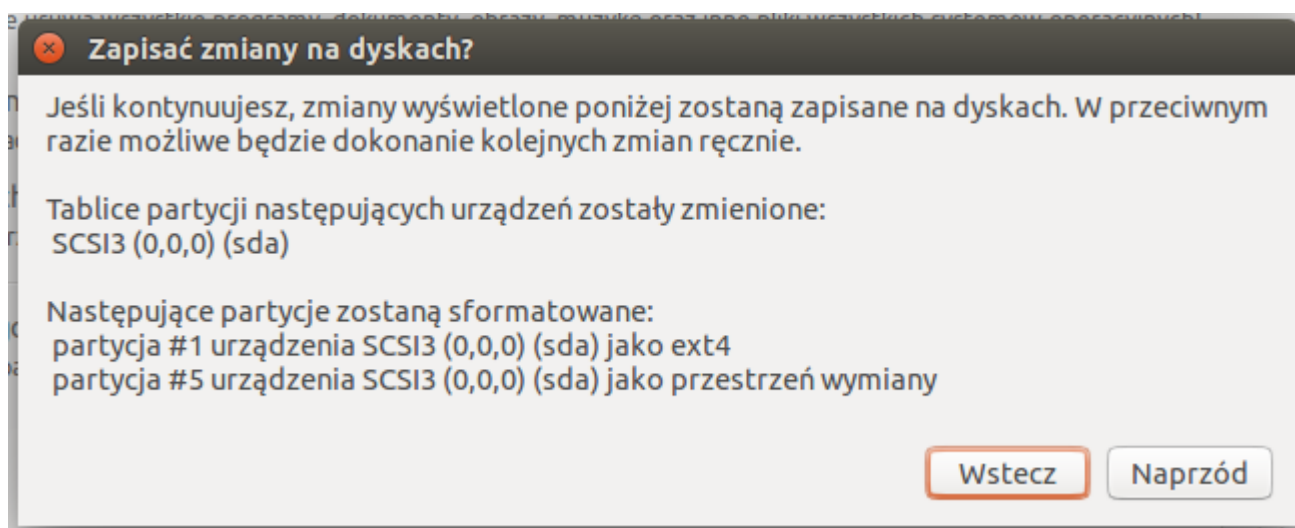
Instalacja systemu na wirtualnej maszynie.



Po przygotowaniu wirtualnej maszyny montujemy w naszym napędzie plik iso z systemem, który będziemy instalować i instalujemy.

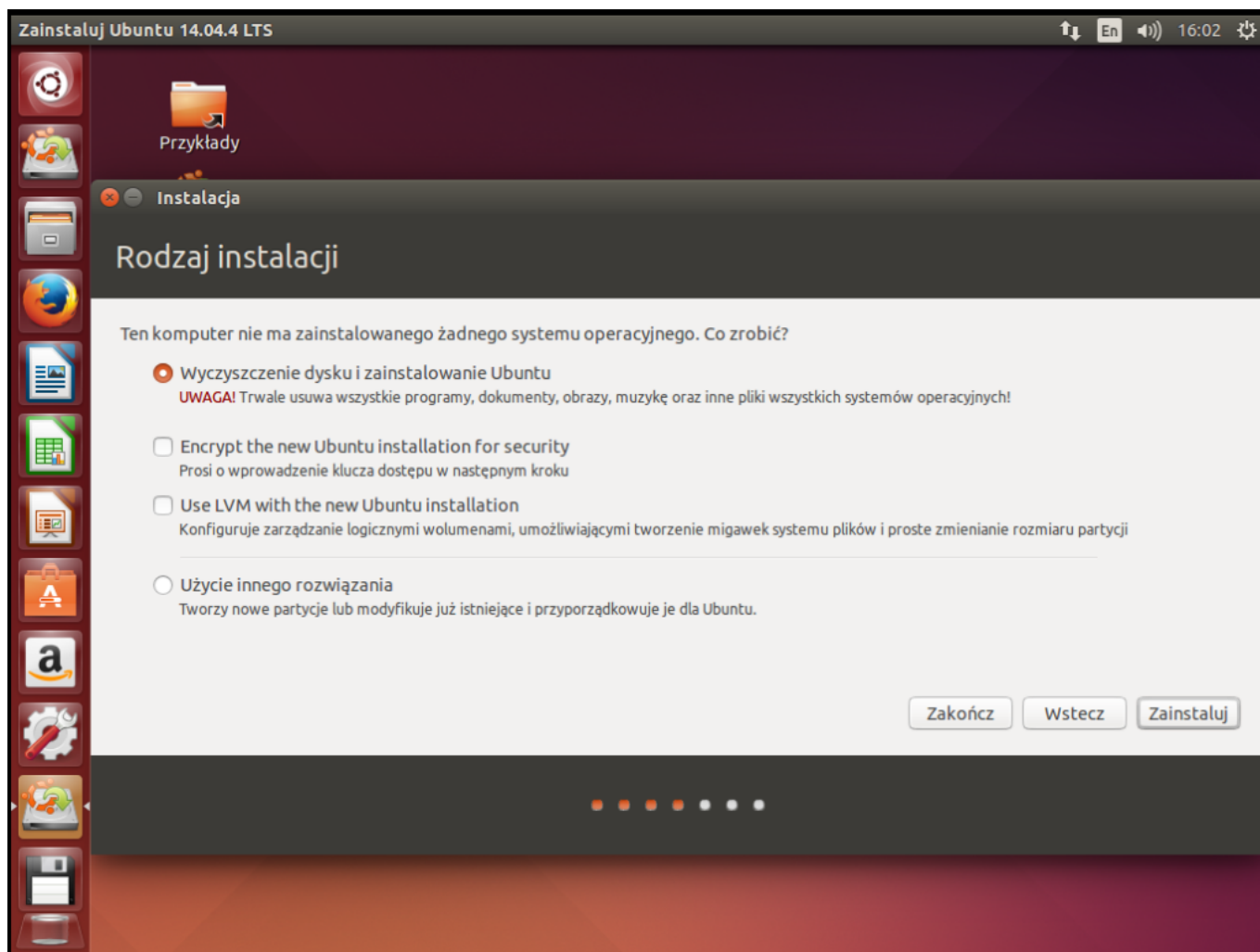


Warto pobrać przy instalacji aktualizacje dla naszego systemu.

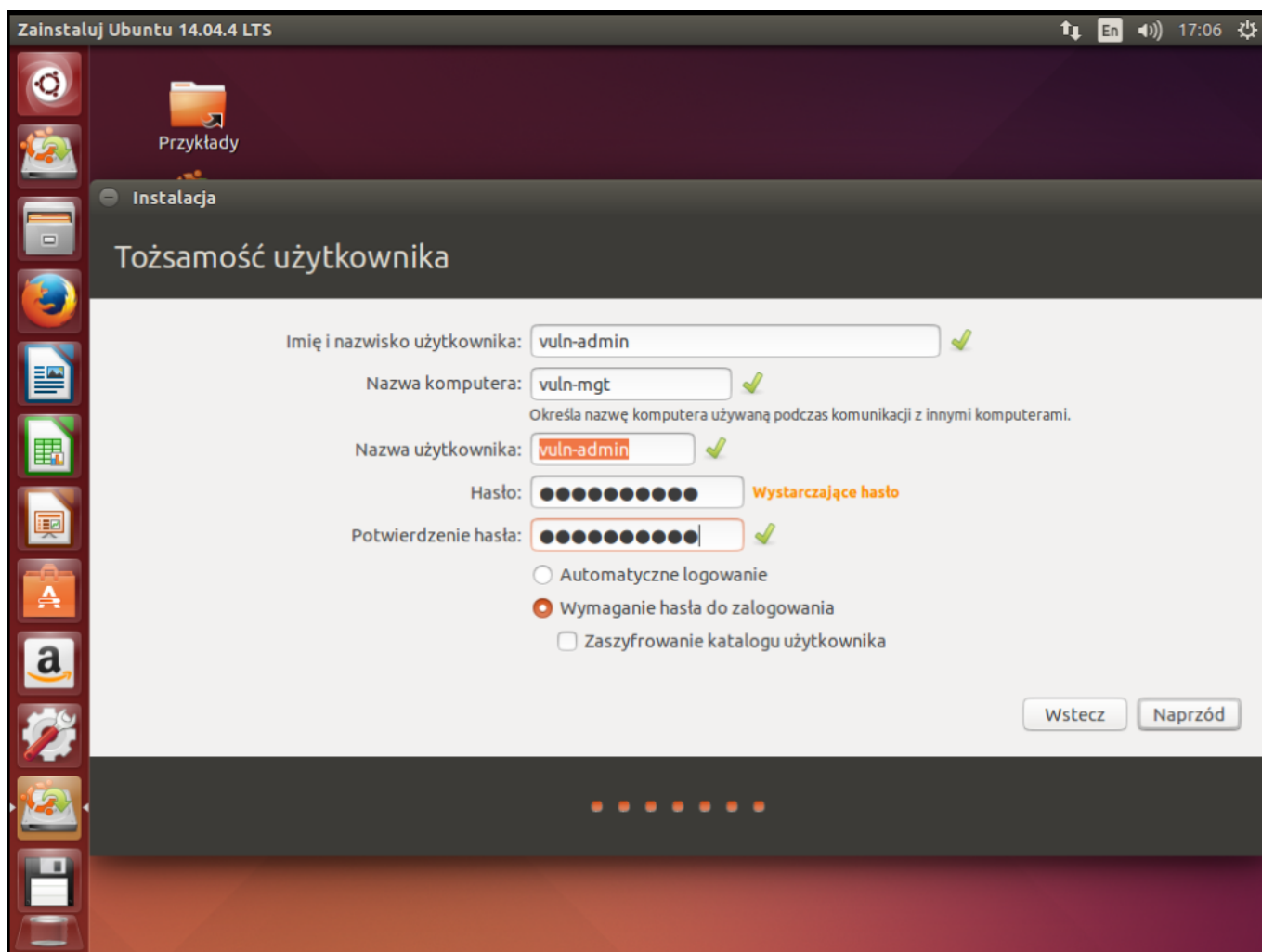


Zap

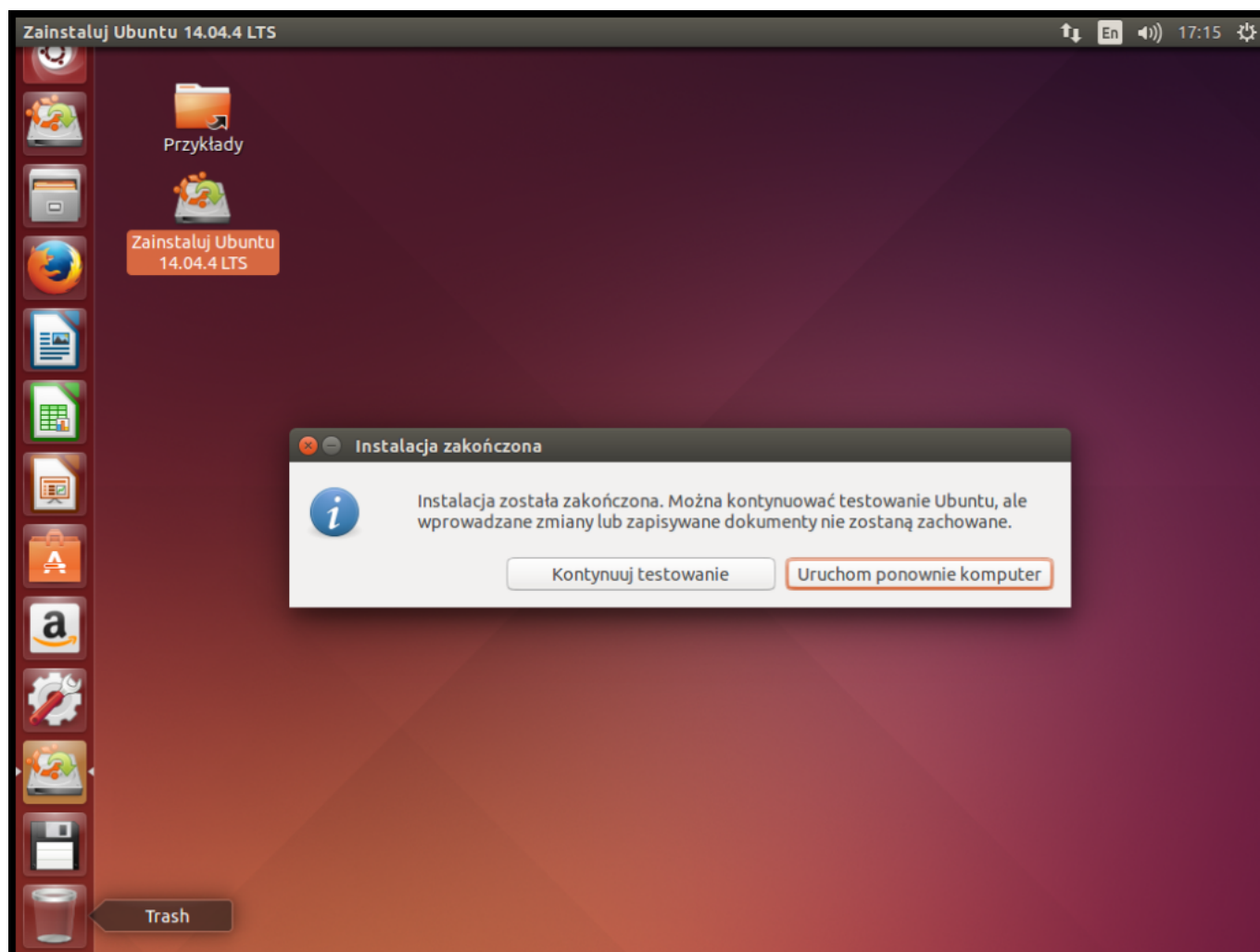
isujemy zmiany na dyskach i przechodzimy dalej.



Rozpoczynamy instalację.



W trakcie instalacji zostaniemy poproszeni o utworzenie użytkownika i określenie hostname naszej maszyny.



Po zakończeniu instalacji, restartujemy maszynę i zabieramy się za instalację Nexpose oraz konfigurację.

Instalacja Nexpose na wirtualnej maszynie.

Za pomocą protokołu SSH łączymy się z maszyną którą przed chwilą zainstalowaliśmy.



```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
pht@dyed-fox:~$ ssh vuln-admin@nexpose.s-m-s.pl
The authenticity of host 'nexpose.s-m-s.pl (172.16.4.5)' can't be established.
ECDSA key fingerprint is SHA256:fDHM6plsaErwPgg5NEykFjgeiE47IW78kEiiZXkuf1E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nexpose.s-m-s.pl,172.16.4.5' (ECDSA) to the list of known ho
sts.
vuln-admin@nexpose.s-m-s.pl's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

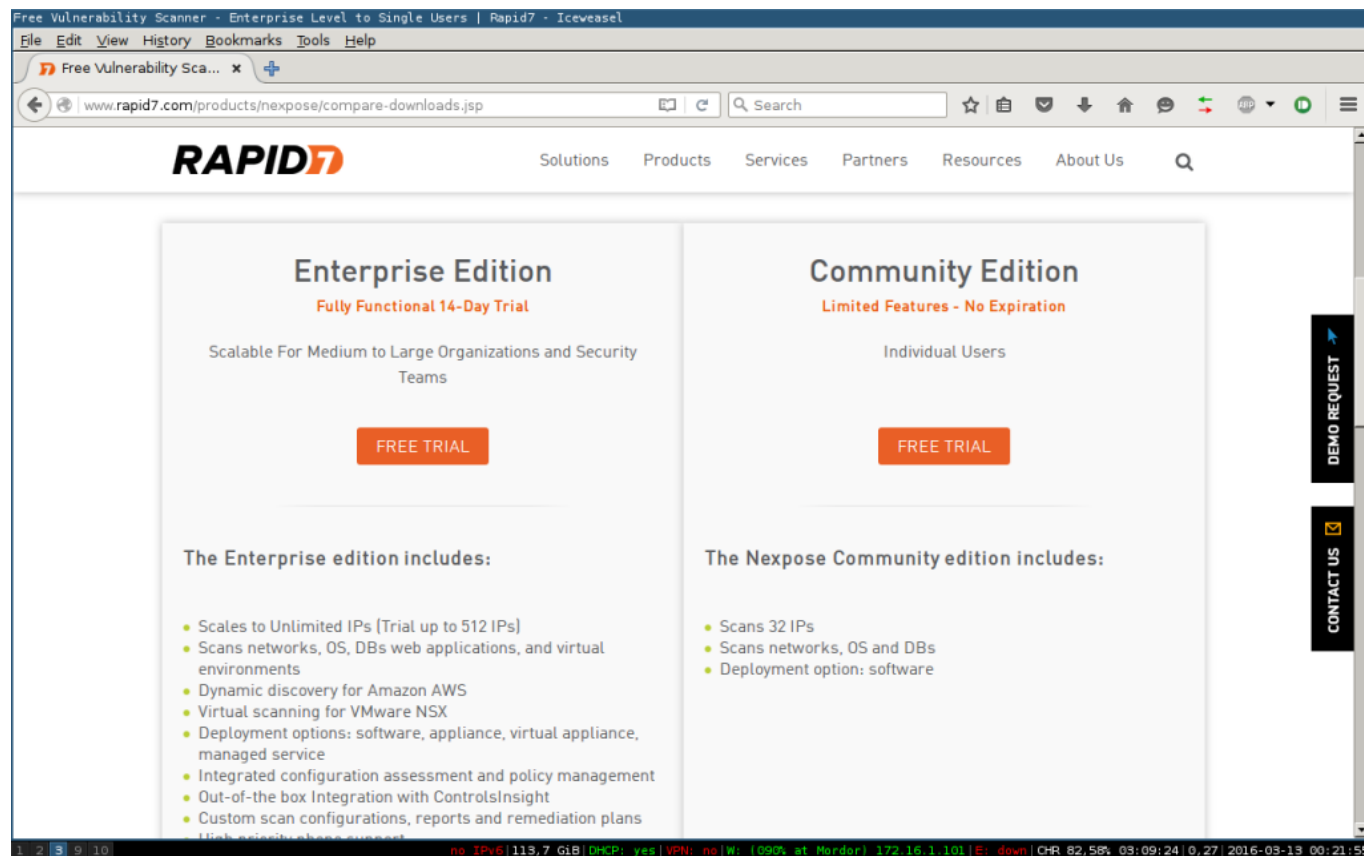
57 packages can be updated.
53 updates are security updates.

Last login: Sat Mar 12 23:45:22 2016 from 172.16.1.101
vuln-admin@vuln-mgt:~$ sudo apt-get update
[sudo] password for vuln-admin:
Ign. http://extras.ubuntu.com trusty InRelease
Pobieranie:1 http://extras.ubuntu.com trusty Release.gpg [72 B]
Stary http://extras.ubuntu.com trusty Release
Stary http://extras.ubuntu.com trusty/main Sources
Stary http://extras.ubuntu.com trusty/main amd64 Packages
Stary http://extras.ubuntu.com trusty/main i386 Packages
Ign. http://extras.ubuntu.com trusty/main Translation-pl_PL
Ign. http://extras.ubuntu.com trusty/main Translation-pl
Ign. http://extras.ubuntu.com trusty/main Translation-en
Ign. http://pl.archive.ubuntu.com trusty InRelease
Pobieranie:2 http://pl.archive.ubuntu.com trusty-updates InRelease [65,9 kB]
Pobieranie:3 http://security.ubuntu.com trusty-security InRelease [65,9 kB]
Pobieranie:4 http://pl.archive.ubuntu.com trusty-backports InRelease [65,9 kB]
Stary http://pl.archive.ubuntu.com trusty Release.gpg
Pobieranie:5 http://pl.archive.ubuntu.com trusty-updates/main Sources [262 kB]
Pobieranie:6 http://security.ubuntu.com trusty-security/main Sources [106 kB]
Pobieranie:7 http://pl.archive.ubuntu.com trusty-updates/restricted Sources [5352 B]
Pobieranie:8 http://pl.archive.ubuntu.com trusty-updates/universe Sources [151 kB]
Pobieranie:9 http://pl.archive.ubuntu.com trusty-updates/multiverse Sources [5946 B]
Pobieranie:10 http://pl.archive.ubuntu.com trusty-updates/main amd64 Packages [713 kB]
Pobieranie:11 http://security.ubuntu.com trusty-security/restricted Sources [4035 B]
Pobieranie:12 http://security.ubuntu.com trusty-security/universe Sources [34,0 kB]
Pobieranie:13 http://security.ubuntu.com trusty-security/multiverse Sources [2750 B]
Pobieranie:14 http://pl.archive.ubuntu.com trusty-updates/restricted amd64 Packages [15,
9 kB]
Pobieranie:15 http://pl.archive.ubuntu.com trusty-updates/universe amd64 Packages [339 k
B]
Pobieranie:16 http://security.ubuntu.com trusty-security/main amd64 Packages [431 kB]
Pobieranie:17 http://pl.archive.ubuntu.com trusty-updates/multiverse amd64 Packages [13,
2 kB]
Pobieranie:18 http://pl.archive.ubuntu.com trusty-updates/main i386 Packages [692 kB]
Pobieranie:19 http://pl.archive.ubuntu.com trusty-updates/restricted i386 Packages [15,6
kB]
Pobieranie:20 http://pl.archive.ubuntu.com trusty-updates/universe i386 Packages [340 kB
]
```

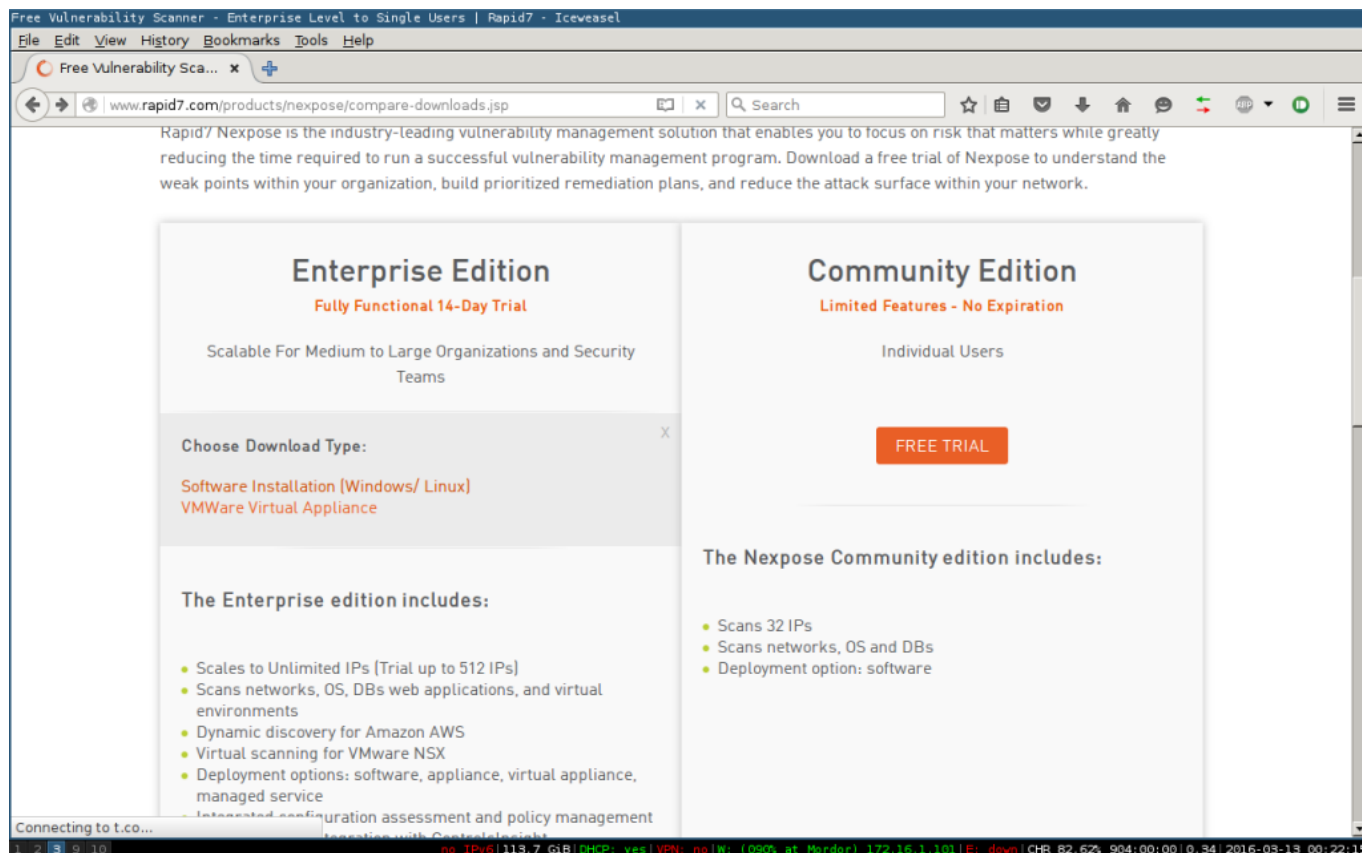
Wyko

nujemy update systemu, dla pewności, że posiadamy najnowsze pakiety.

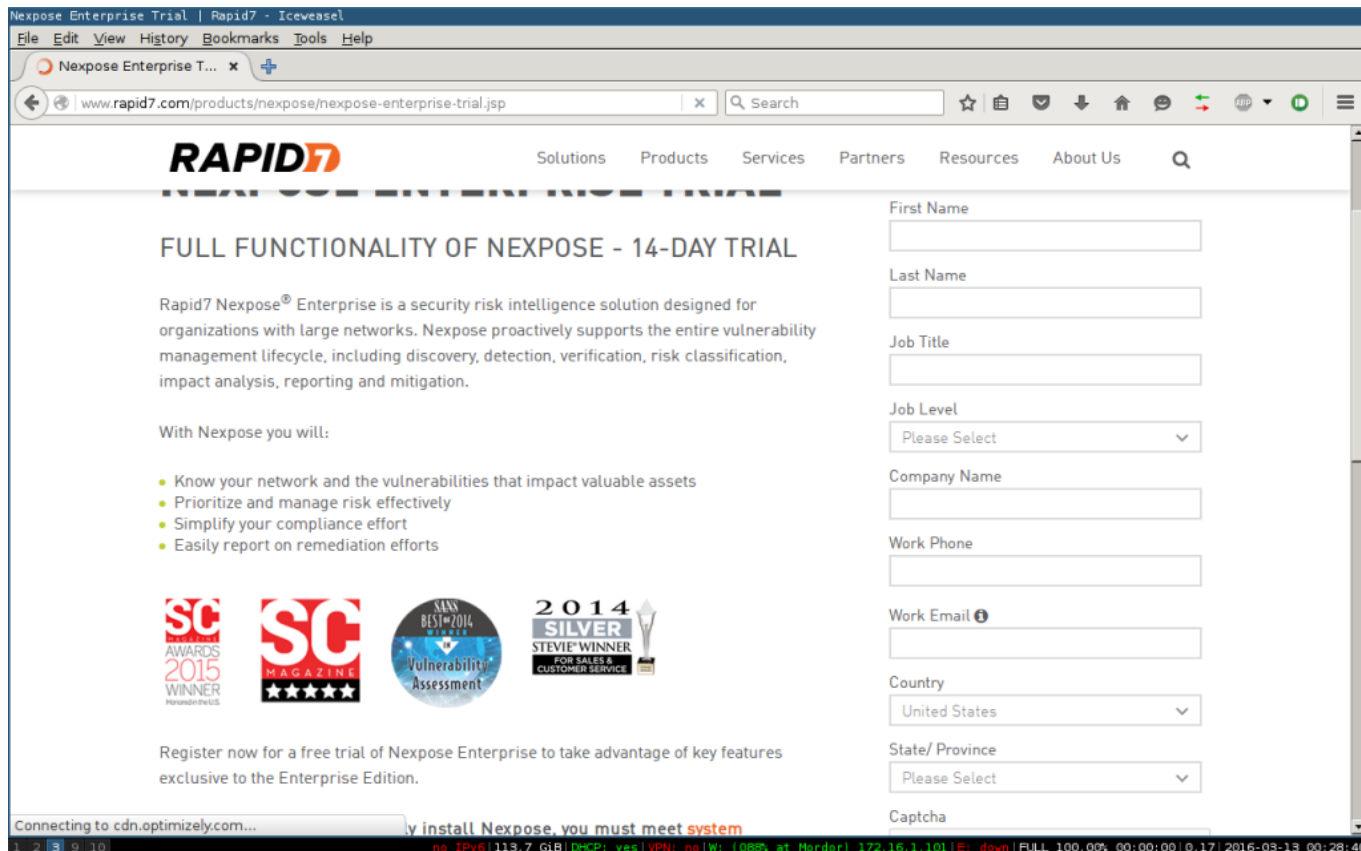
Z strony Rapid7 pobieramy plik instalacyjny Nexpose. Na potrzeby artykułów, aby pokazać pełen zakres możliwości, pobieramy wersję „Enterprise”.



Wybieramy „Software Installation”, możemy również pobrać już gotowy obraz wirtualnej maszyny i wgrać go do naszego serwera wirtualizacji.



Następnym krokiem jaki musimy wykonać to wypełnienie krótkiego formularza rejestracyjnego, który zapewni nam darmową dwutygodniową licencję.



Nexpose Enterprise Trial | Rapid7 - Iceveasel

File Edit View History Bookmarks Tools Help

Nexpose Enterprise T... x

www.rapid7.com/products/nexpose/nexpose-enterprise-trial.jsp

RAPID7

Solutions Products Services Partners Resources About Us

FULL FUNCTIONALITY OF NEXPOSE - 14-DAY TRIAL

Rapid7 Nexpose® Enterprise is a security risk intelligence solution designed for organizations with large networks. Nexpose proactively supports the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation.

With Nexpose you will:

- Know your network and the vulnerabilities that impact valuable assets
- Prioritize and manage risk effectively
- Simplify your compliance effort
- Easily report on remediation efforts

Register now for a free trial of Nexpose Enterprise to take advantage of key features exclusive to the Enterprise Edition.

First Name

Last Name

Job Title

Job Level

Company Name

Work Phone

Work Email

Country

State/ Province

Captcha

SC AWARDS 2015 WINNER

SC MAGAZINE

2014 SILVER STEVIE WINNER FOR SALES & CUSTOMER SERVICE

2014 BEST IN CLASS Vulnerability Assessment

Connecting to cdn.optimizely.com... y install Nexpose, you must meet system

no IPv6 | 119,7 GiB | DHCP: yes | VPN: no | W: 1088p at Nordar | 172.16.1.101 | E: down | FULL 100,00% 00:00:00 0,17 | 2016-05-13 00:28:40

Wybieramy wersję pliku instalacyjnego względem systemu na maszynie na której będziemy instalować Nexpose.



Nexpose Enterprise | Rapid7 - Iceweasel

File Edit View History Bookmarks Tools Help

Nexpose Enterprise | ... x

www.rapid7.com/products/nexpose/nexpose-enterprise-trial-thank-you.jsp?whence=

RAPID7 Solutions Products Services Partners Resources About Us

Next steps to get started with Nexpose Enterprise trial

STEP 1: Download

Windows	Ubuntu	Red Hat Enterprise Linux
64-Bit md5sum	64-Bit md5sum	64-Bit md5sum

STEP 2: Install

Once the download is complete, run the installer and follow the step by step instructions.

STEP 3: Activate

Need help?

Here are some resources to help you.

- Did you not receive your license key? Please check your spam folder.
- Ask Questions: [Join Nexpose Community on SecurityStreet](#)
- Download: [Nexpose Quickstart guide](#)
- Activation problems: [Download our Nexpose activation troubleshooting guide](#)
- Other Issues: [Contact info@rapid7.com](#)

no IPv6 | 119,7 GiB | DHCP: yes | VPN: no | W: 105% at Nordar | 172.16.1.101 | E: down | FULL 100,00% 00:00:00 0,55 | 2016-05-13 00:29:50

Klikamy prawym na link do pliku instalacyjnego i kopiujemy jego wartość. Użyjemy tego do pobrania instalki na naszą maszynę.



```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
vuln-admin@vuln-mgt:~$ wget http://download2.rapid7.com/download/NeXpose-v4/NeXposeSetup-Linux64.bin
--2016-03-13 00:38:05--  http://download2.rapid7.com/download/NeXpose-v4/NeXposeSetup-Linux64.bin
Translacja download2.rapid7.com (download2.rapid7.com)... 23.61.248.75, 23.61.248.67
Łączenie się z download2.rapid7.com (download2.rapid7.com)|23.61.248.75|:80... połączono
.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... 200 OK
Długość: 694295704 (662M) [application/octet-stream]
Zapis do: `NeXposeSetup-Linux64.bin'

100%[=====>] 694.295.704 6,44MB/s   w 1m 51s

2016-03-13 00:39:57 (5,97 MB/s) - zapisano `NeXposeSetup-Linux64.bin' [694295704/694295704]

vuln-admin@vuln-mgt:~$ chmod +x NeXposeSetup-Linux64.bin
vuln-admin@vuln-mgt:~$ ls
examples.desktop  NeXposeSetup-Linux64.bin
vuln-admin@vuln-mgt:~$
```

Za pomocą narzędzia wget pobieramy, po czym nadajemy mu uprawnienia do wykonywania.



Uruchamiamy instalację jako root i postępujemy zgodnie z dalszymi instrukcjami.

```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
[sudo] password for vuln-admin:
Unpacking JRE ...
Starting Installer ...
mar 13, 2016 1:33:20 AM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
mar 13, 2016 1:33:20 AM java.util.prefs.FileSystemPreferences$2 run
INFO: Created system preferences directory in java.home.

*****
Welcome to the Nexpose Installation Wizard
*****

Rapid7 Nexpose identifies vulnerabilities in networks, operating systems,
databases, programs, and Web applications. Prioritizing these
vulnerabilities with exploit risk scoring and asset criticality ratings,
Nexpose helps your organization reduce risk exposure and remediation costs.

Rapid7, LLC
http://www.rapid7.com
info@rapid7.com
+1.866.772.7437
+1.617.247.1717

Do you want to continue?
Yes [y, Enter], No [n]
y

Gathering system information...

*****
Scroll through and read the agreement to accept it
*****

Rapid7 End User License and Services Terms and Conditions

Customer agrees to be bound by the following terms and conditions (this "Agreement") in
connection with its purchase and use of certain Rapid7 LLC's ("Rapid7") Software and Ser
vices (each as defined below). Before installing and using any Software and/or obtaining
and using any Services you should read this Agreement carefully. Clicking "accept" or o
therwise installing and/or using the Software and/or obtaining and/or using any Services
establishes a binding agreement between Rapid7 and you as the person licensing the Soft
ware and/or obtaining the Services; provided that if you are entering into this Agreemen
t on behalf of a company or other legal entity, you represent that you have the authorit
y to bind such entity to this Agreement, in which case the term "Customer" shall refer t
o such entity. If you do not have such authority or if you do not accept all of the term
s of this Agreement, you shall have no right to install and/or use the Software and/or o
btain and/or use any Services.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
█
```



Plik Edycja Widok Wyszukiwanie Terminal Pomoc

rnment agrees to return the Software, unused, to Rapid7. Manufacturer is Rapid7 LLC, 100 Summer Street, Boston, MA 02110.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

12.6. Relationship of the Parties. Rapid7 and Customer are independent contractors, and nothing in this Agreement shall be construed as making them partners or creating the relationships of employer and employee, master and servant, or principal and agent between them, for any purpose whatsoever. Neither party shall make any contracts, warranties or representations or assume or create any obligations, express or implied, in the other party's name or on its behalf.

12.7. Force Majeure. Except for the obligation to make payments, nonperformance of either party shall be excused to the extent that performance is rendered impossible by strike, fire, flood, governmental acts or orders or restrictions, failure of suppliers, or any other reason where failure to perform is beyond the reasonable control of the non-performing party.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

12.8. No reliance. Customer represents that it has not relied on the availability of any future version of the purchased product or any future product in executing this Agreement or placing any orders hereunder.

12.9. Third Party Software. Customer acknowledges that the Software may contain or be accompanied by certain third party hardware and software products or components ("Third-Party Products"). Additional information about Third-Party Products may be set forth in the Product Order Form, the Third Party Product packaging and/or in a text file, installation file or similar file or folder accompanying the Software ("Third-Party Notices"). The Third-Party Notices may include important licensing and warranty information and disclaimers. Customer acknowledges that Section 10 of this Agreement shall not be applicable to the Third-Party Products.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

12.10. Publicity. Customer acknowledges that Rapid7 may use Customer's name and logo for the purposes of identifying Customer as a customer of Rapid7 products and/or services, including in Rapid7's quarterly press releases highlighting new customer engagements.

12.11. Notices. Any demand, notice, consent, or other communication required by this Agreement must be given in writing and shall be deemed delivered upon receipt when delivered personally or upon confirmation of receipt following delivery by a nationally recognized overnight courier service, in each case addressed to the receiving party at its address set forth on the applicable Product Order Form. Either party may change its address by giving written notice of such change to the other party.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

Do you accept the license?

1. I accept the agreement. [1]
2. I do not accept the agreement. [2, Enter]
3. Cancel [3]



Plik Edycja Widok Wyszukiwanie Terminal Pomoc

e, fire, flood, governmental acts or orders or restrictions, failure of suppliers, or any other reason where failure to perform is beyond the reasonable control of the non-performing party.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

12.8. No reliance. Customer represents that it has not relied on the availability of any future version of the purchased product or any future product in executing this Agreement or placing any orders hereunder.

12.9. Third Party Software. Customer acknowledges that the Software may contain or be accompanied by certain third party hardware and software products or components ("Third-Party Products"). Additional information about Third-Party Products may be set forth in the Product Order Form, the Third Party Product packaging and/or in a text file, installation file or similar file or folder accompanying the Software ("Third-Party Notices"). The Third-Party Notices may include important licensing and warranty information and disclaimers. Customer acknowledges that Section 10 of this Agreement shall not be applicable to the Third-Party Products.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

12.10. Publicity. Customer acknowledges that Rapid7 may use Customer's name and logo for the purposes of identifying Customer as a customer of Rapid7 products and/or services, including in Rapid7's quarterly press releases highlighting new customer engagements.

12.11. Notices. Any demand, notice, consent, or other communication required by this Agreement must be given in writing and shall be deemed delivered upon receipt when delivered personally or upon confirmation of receipt following delivery by a nationally recognized overnight courier service, in each case addressed to the receiving party at its address set forth on the applicable Product Order Form. Either party may change its address by giving written notice of such change to the other party.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

Do you accept the license?

1. I accept the agreement. [1]
2. I do not accept the agreement. [2, Enter]
3. Cancel [3]

1

Nexpose Security Console with local Scan Engine

If you do not have a console installed yet, this option is recommended. The console manages scan engines and all Nexpose operations.

Nexpose Scan Engine only

This distributed engine can start scanning after being paired with a Nexpose Security Console.

Select only the set of components you want to install:

Nexpose Security Console with local Scan Engine [1, Enter]

Nexpose Scan Engine only [2]



```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
ed personally or upon confirmation of receipt following delivery by a nationally recogni
zed overnight courier service, in each case addressed to the receiving party at its addr
ess set forth on the applicable Product Order Form. Either party may change its address
by giving written notice of such change to the other party.

Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]

Do you accept the license?
1. I accept the agreement. [1]
2. I do not accept the agreement. [2, Enter]
3. Cancel [3]
1

Nexpose Security Console with local Scan Engine
If you do not have a console installed yet, this option is recommended. The console mana
ges scan engines and all Nexpose operations.

Nexpose Scan Engine only
This distributed engine can start scanning after being paired with a Nexpose Security Co
nsole.

Select only the set of components you want to install:
Nexpose Security Console with local Scan Engine [1, Enter]
Nexpose Scan Engine only [2]

Where should Nexpose be installed?
[/opt/rapid7/nexpose]

*****
The installer is comparing your system settings to required settings
*****

Hardware requirements
[Pass] - AMD 8 Core(s) @ 3,515 MHz processor was detected.
[Warn] - 3,952 MB RAM was detected. 8,192 MB RAM is recommended.
Software requirements
[Pass] - Ubuntu 14.04 operating system was detected.
[Pass] - SELinux is not active.
[Pass] - Nexpose is not running.
Ports and connectivity
Not checked.
[Pass] - Port 3780 is available.
[Pass] - Access to external networks was detected.

Minimum requirements met. Select "Yes" to continue, "No" to cancel installation.
Yes [y, Enter], No [n]
█
```



```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
*****
The installer is comparing your system settings to required settings
*****

Hardware requirements
[Pass] - AMD 8 Core(s) @ 3,515 MHz processor was detected.
[Warn] - 3,952 MB RAM was detected. 8,192 MB RAM is recommended.
Software requirements
[Pass] - Ubuntu 14.04 operating system was detected.
[Pass] - SELinux is not active.
[Pass] - Nexpose is not running.
Ports and connectivity
Not checked.
[Pass] - Port 3780 is available.
[Pass] - Access to external networks was detected.

Minimum requirements met. Select "Yes" to continue, "No" to cancel installation.
Yes [y, Enter], No [n]

*****
Enter your first and last names, and the name of your company. This information will be
used for generating SSL certificates, and it will be included in requests to Technical S
upport. Only alphanumeric characters and spaces are allowed in the name fields.
*****

First name:
[]
Piotr
Last name:
[]
Jasiek
Company:
[]
S.M.S
Database port
Enter the number for the port that the database will listen on:
[5432]

The port number is valid.

*****
IMPORTANT: Choose secure credentials and remember them. You will need them to perform co
nfiguration steps after completing the installation.
*****

User name:
[]
█
```




```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
Database port
Enter the number for the port that the database will listen on:
[5432]

The port number is valid.

*****
IMPORTANT: Choose secure credentials and remember them. You will need them to perform co
nfiguration steps after completing the installation.
*****

User name:
[]
pht

Password:

Confirm the password:

Password match confirmed.

*****
Confirm or change your installation selections
*****

*****
Additional Tasks Selection
*****

You have selected the following installation location:
/opt/rapid7/nexpose

You have selected the following component(s) to install:
Nexpose Security Console, Nexpose Scan Engine

You have entered the following contact information:
Piotr Jasiek, S.M.S

You have created the following user name:
pht

Select any additional installation tasks.
Initialize and start Nexpose after installation?
Yes [y], No [n, Enter]

```



```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc

You have selected the following component(s) to install:
Nexpose Security Console, Nexpose Scan Engine

You have entered the following contact information:
Piotr Jasiek, S.M.S

You have created the following user name:
pht

Select any additional installation tasks.
Initialize and start Nexpose after installation?
Yes [y], No [n, Enter]

*****
Extracting files...
*****

Extracting files...

*****
Installation is complete!
*****

Installation is complete!

If you chose to start Nexpose as part of the installation, then it is already running.

Using the credentials you created during installation, log onto Nexpose at https://local
host:3780.

To start scanning, click the *Home* tab in the Nexpose Security Console Web interface. F
or quick-start help, click the *Help* link.

You can start Nexpose manually by executing
/opt/rapid7/nexpose/nsc/nsc.sh.

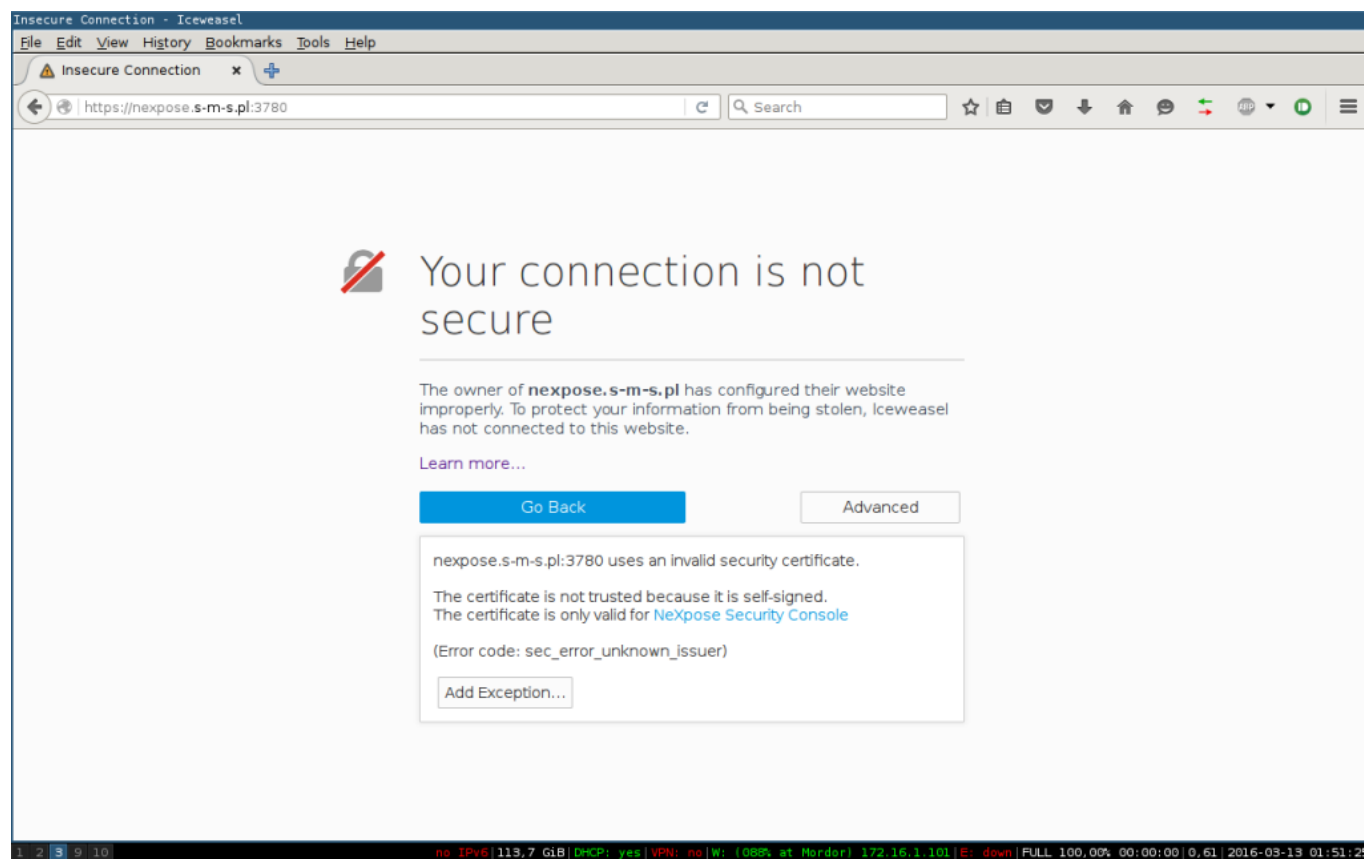
NOTE: If you did not select the option to start Nexpose as part of the installation, Nex
pose will take 10 to 30 minutes to initialize during first-time startup depending on you
r system capabilities.

Nexpose is configured to start automatically. See the installation guide if you wish to
modify start modes.

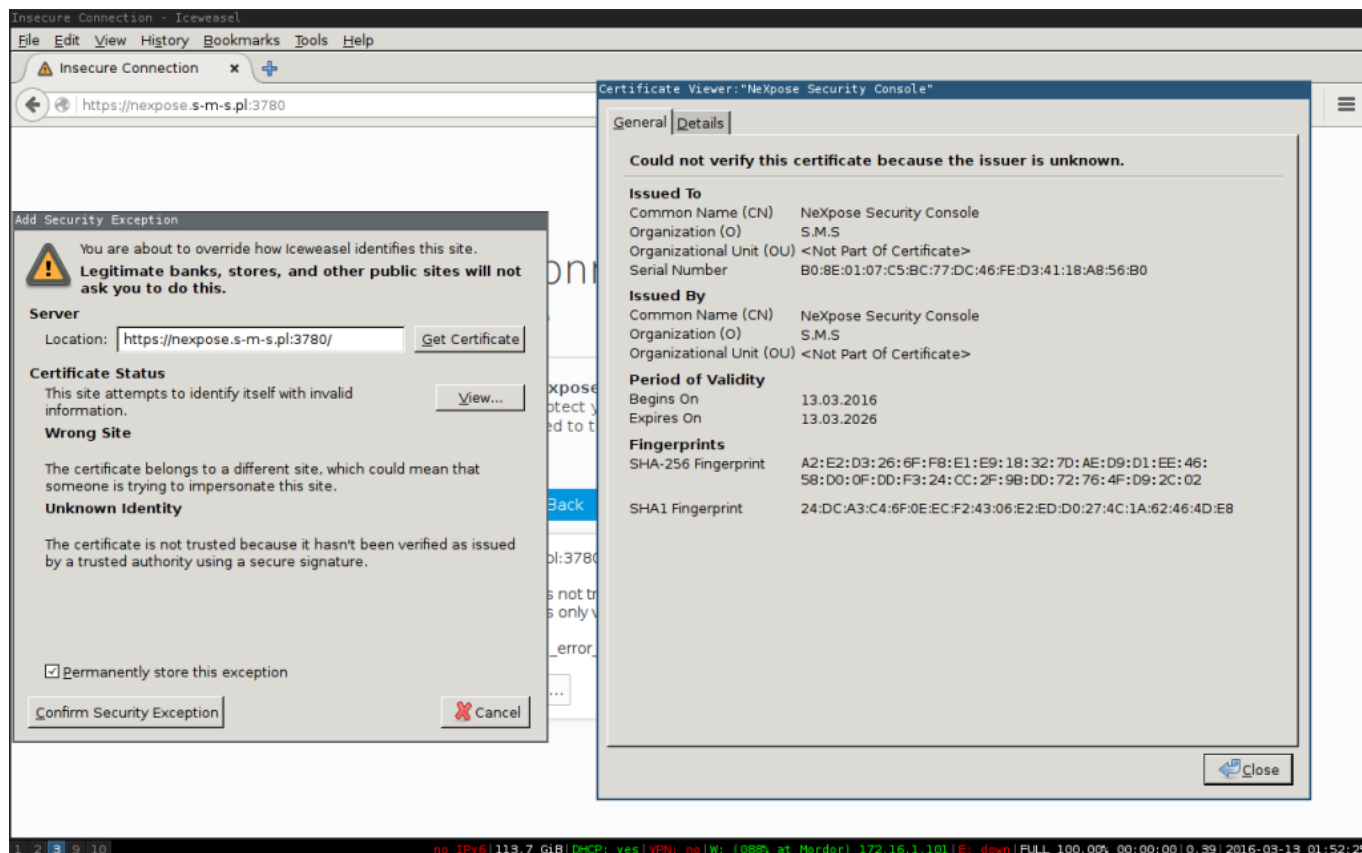
[Enter]
```

Konfiguracja z poziomu webpanelu.

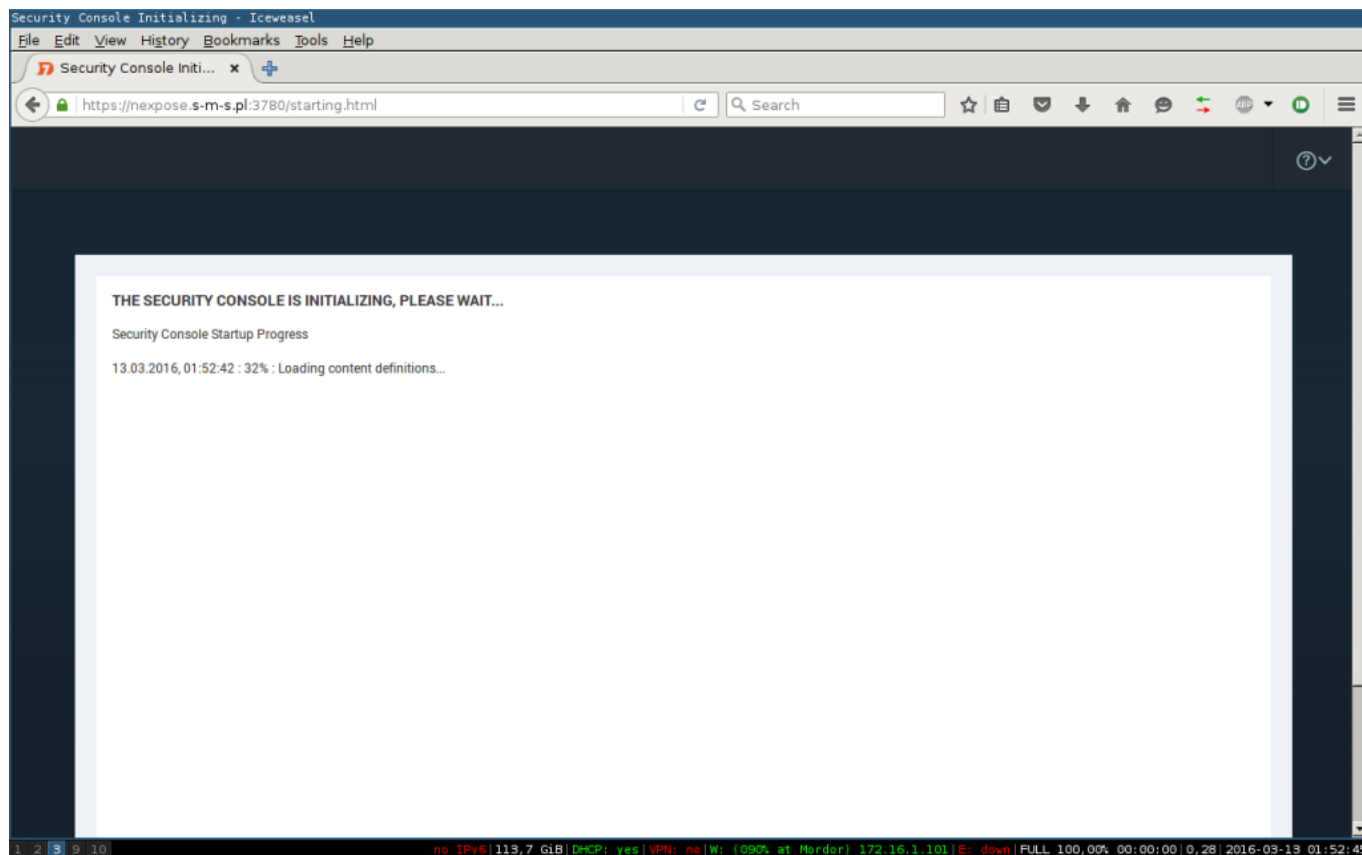
Następnie przechodzimy do web-panelu. W naszym przypadku panel znajduje się pod adresem <https://nexpose.s-m-s.pl:3780>.



Jak widzimy nasz panel identyfikuje się certyfikatem SSL typu „self-signed”.



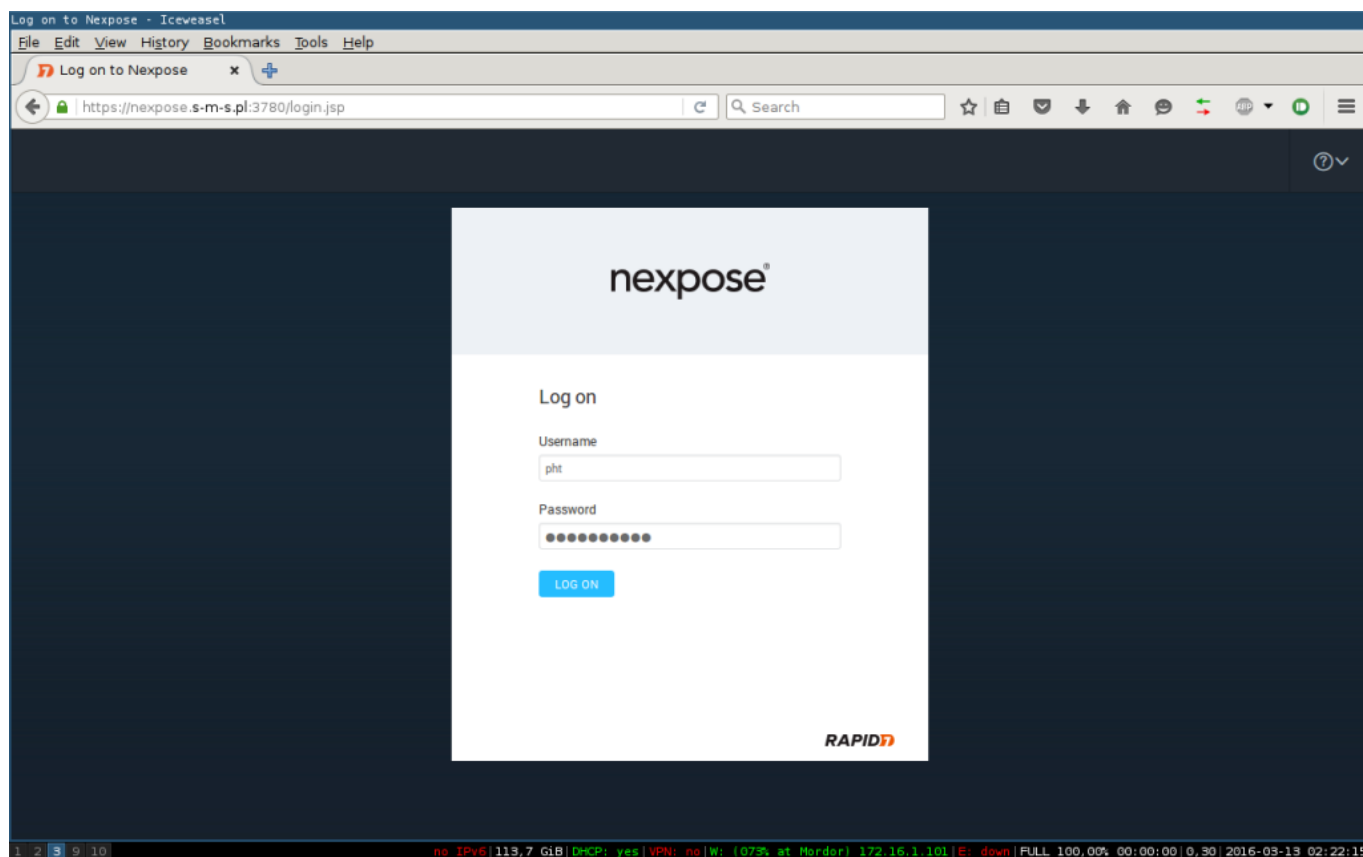
Sprawdzamy, czy przedstawiony certyfikat na pewno jest tym, który wygenerowaliśmy podczas instalacji i dodajemy wyjątek bezpieczeństwa.



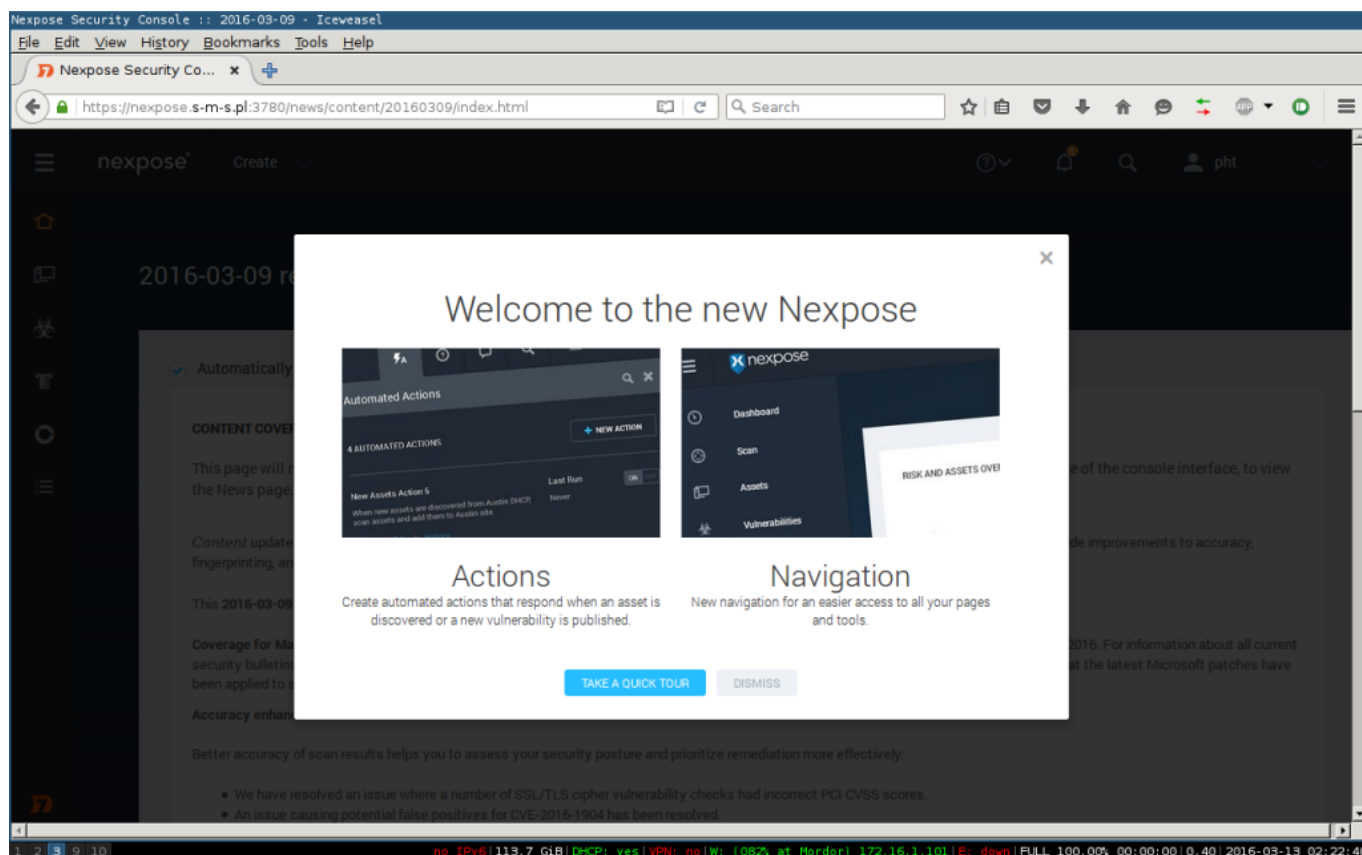
Pierwsze uruchomienie może trwać od 10 do 30 minut, jest to zależne jakimi zasobami pamięci dysponuje maszyna na której zainstalowaliśmy Nexpose. Według vendora minimalna ilość pamięci RAM to 8 GB, my daliśmy 4 GB. Do działań laboratoryjnych owe 4 GB starczy bez problemu, natomiast, do seryjnej pracy zaleca się, aby maszyna na której będzie instalowany Nexpose miała 8 GB i więcej RAM-u.



Nexpose - Wstępna konfiguracja

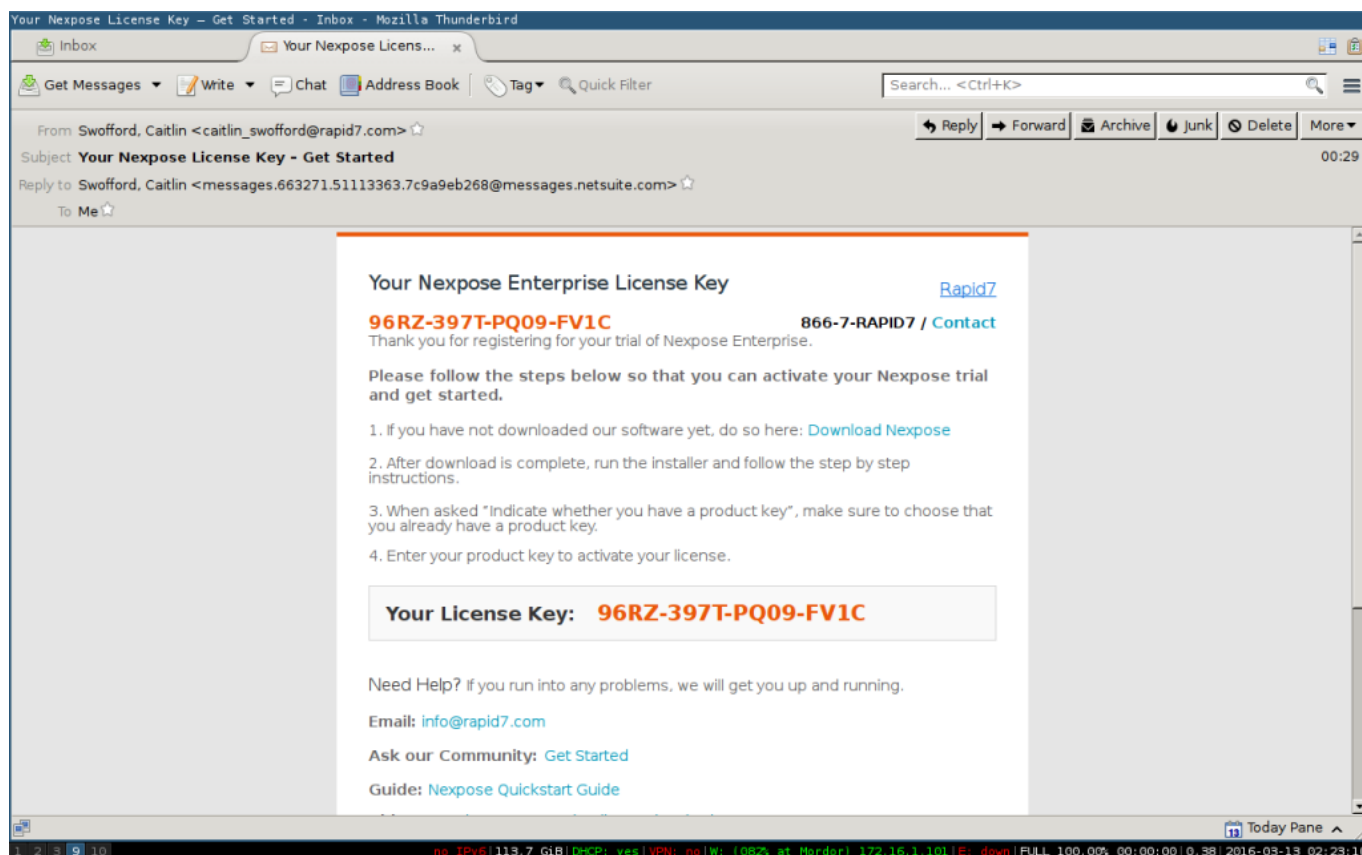


Podczas instalacji podaliśmy login i hasło dla nowego użytkownika. Czas skorzystać z tych danych.



Możemy skorzystać z wbudowanego samouczka, który oprowadzi nas po panelu Nexpose i pokaże co i gdzie możemy znaleźć.

Po zalogowaniu również zostaniemy poproszeni o podanie klucza licencyjnego. Jeżeli podaliśmy prawidłowy email podczas rejestracji, powinniśmy mieć na nim maila od Rapid7 z licencją.



Przypominamy, że licencja, którą otrzymujemy na maila po rejestracji na stronie Rapid7 jest darmowa i ograniczona czasowo. Trwa ona 14 dni. Po zakończeniu licencji, możemy odnowić licencje, korzystając z tych samych danych co poprzednio.



Nexpose - Wstępna konfiguracja

Nexpose Security Console :: 2016-03-09 - Iceveasel

File Edit View History Bookmarks Tools Help

Nexpose Security Co... x

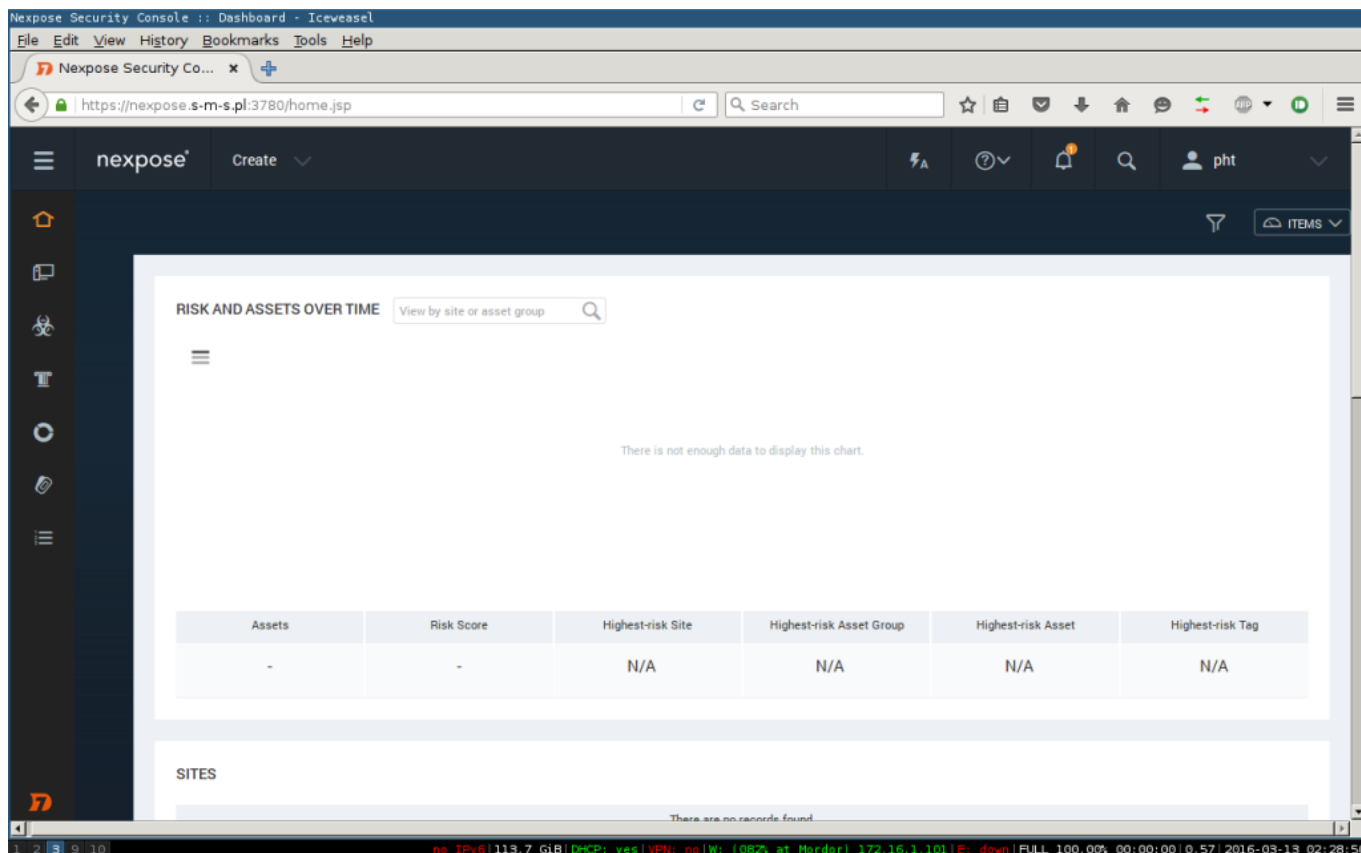
https://nexpose.s-m-s.pl:3780/news/content/20160309/index.html

Activate License

You need an active license for scanning and reporting. To activate...

Activating the Security Console. Please wait...

no IPv6 | 119,7 GiB | DHCP: yes | VPN: no | W: (86% at Morder) 172.16.1.101 | E: down | FULL 100,00% 00:00:00 0,11 | 2016-03-13 02:25:10



Po zakończeniu aktywacji przed naszymi oczami ukazuje się gotowy panel. To wszystko jeżeli chodzi o konfigurację samego oprogramowania w przypadku manualnej instalacji.

Poprawki bezpieczeństwa.

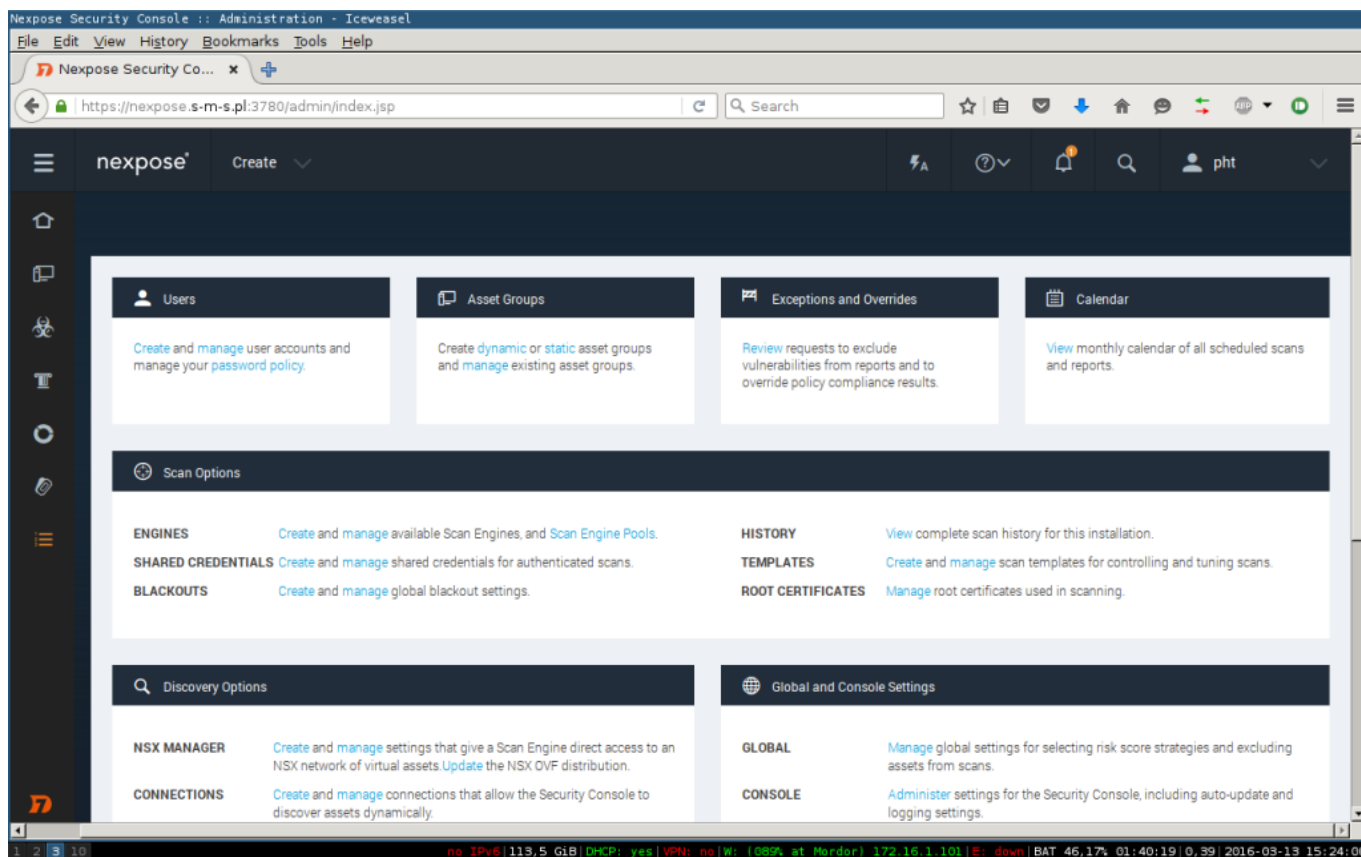
Jeżeli ktoś wybrał instalację z gotowego obrazu maszyny wirtualnej, powinien pamiętać o kilku, istotnych rzeczach. Pierwszą z nich jest fakt, iż domyślnymi danymi dostępowymi są:

- dla OS: nexpose:nexpose
- dla samego web panelu: nxadmin:nxpassword

Dane te, należy niezwłocznie zmienić zaraz po zakończeniu powyższych czynności.

Aby zmienić dane dostępowe do panelu Nexpose, możemy zrobić to na dwa sposoby. Dodać nowego użytkownika i zablokować domyślnego, lub po prostu zmienić hasło dla domyślnego

usera. Działania te wykonujemy w zakładce „Administracja”



By utworzyć użytkownika, wybieramy „Create” w zakładce „Users”.



Nexpose - Wstępna konfiguracja

Nexpose Security Console :: User Configuration - Iceweasel

File Edit View History Bookmarks Tools Help

Nexpose Security Co... x

https://nexpose.s-m-s.pl:3780/admin/user/config.jsp

nexpose Create

User Configuration

SAVE CANCEL

GENERAL

Enter information that will identify this user. Select an authentication method if more than one is available. Consult your network administrator about multiple authentication options. This user cannot access the Security Console unless you select the check box to enable the account. You can clear the check box at any time to take away access.

User name: nowy

Authentication method: Nexpose user

Full name: Nowy User

E-mail address: nowy@domena.pl

Password: [masked]

Confirm password: [masked]

Account enabled

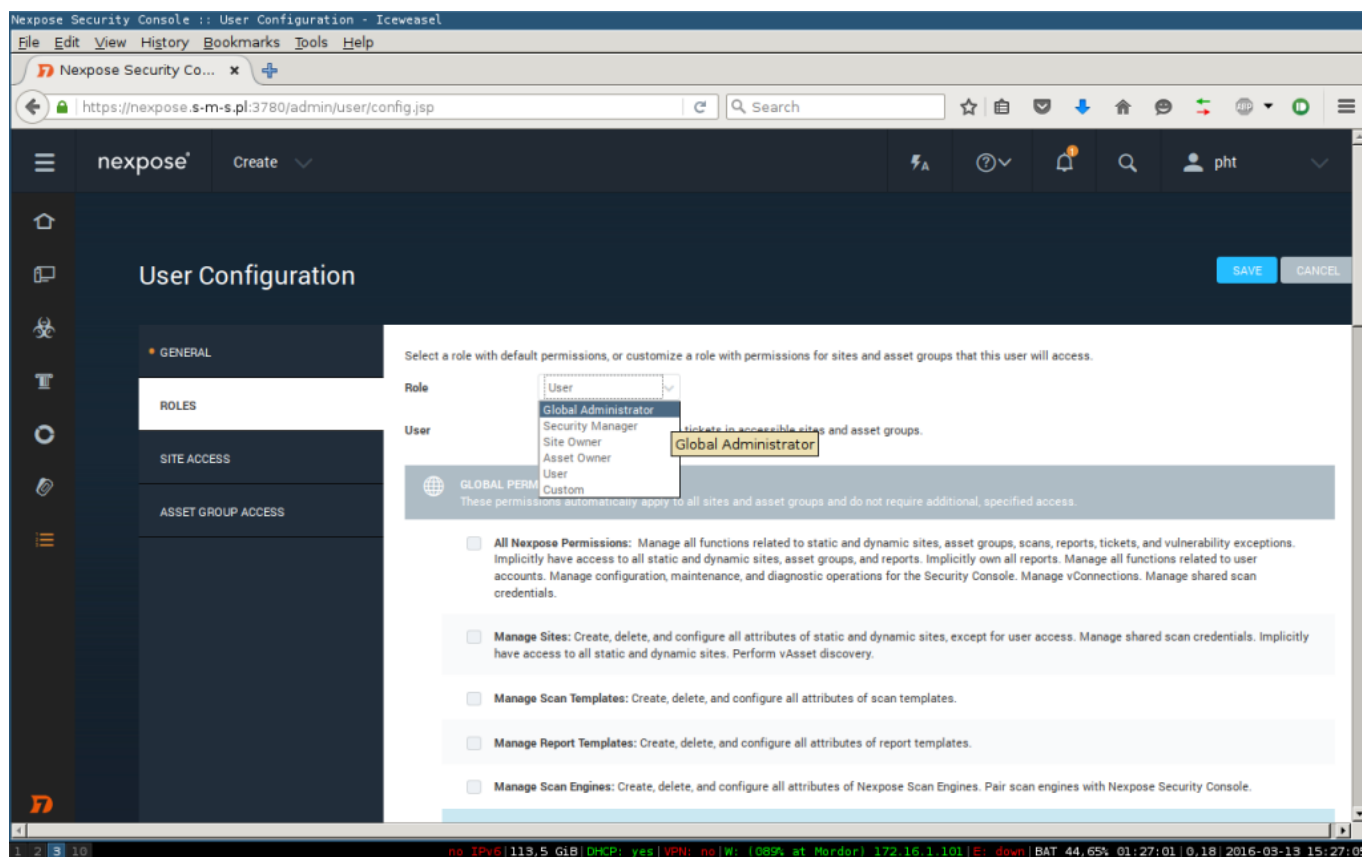
Require password reset upon login

ROLES

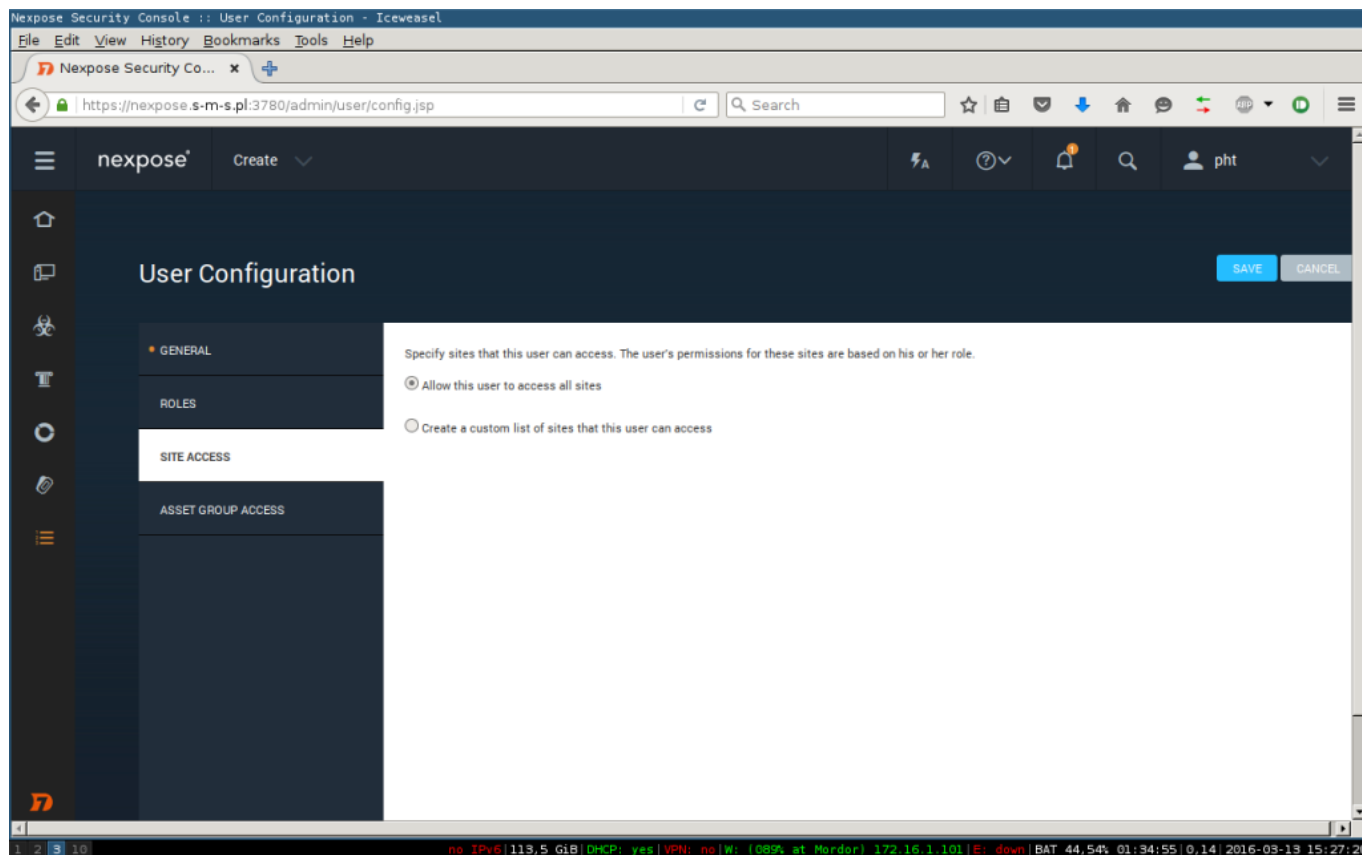
SITE ACCESS

ASSET GROUP ACCESS

no IPv6 | 113,5 GiB | DHCP: yes | VPN: no | W: 100% at Mordor | 172.16.1.101 | E: down | BAT 44,94% | 01:39:22 | 0,52 | 2016-03-13 15:26:30



Wybieramy rodzaj uprawnień nowego użytkownika. Możemy skorzystać z gotowych szablonów lub stworzyć własny zakres uprawnień. Zachęcamy do zapoznania się z listą uprawnień.



Wybieramy dostęp do działów „site” oraz „asset group” o których więcej napiszemy w następnym artykule z serii.



Nexpose - Wstępna konfiguracja

Nexpose Security Console :: User Configuration - Iceweasel

File Edit View History Bookmarks Tools Help

Nexpose Security Co... x

https://nexpose.s-m-s.pl:3780/admin/user/config.jsp

nexpose Create

Home

User Configuration

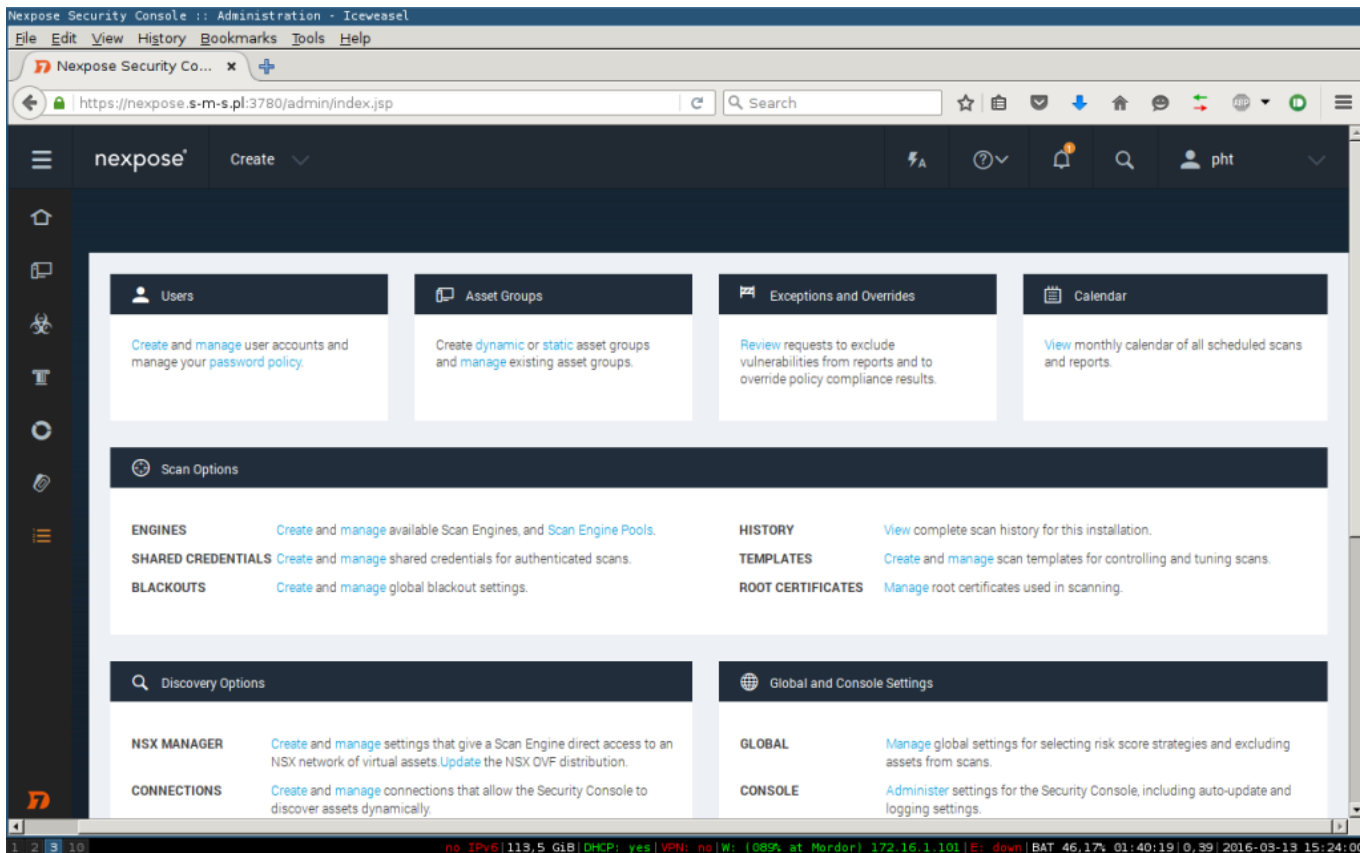
SAVE CANCEL

- GENERAL
- ROLES
- SITE ACCESS
- ASSET GROUP ACCESS

Specify asset groups that this user can access. The user's permissions for these asset groups are based on his or her role.

- Allow this user to access all asset groups
- Create a custom list of asset groups that this user can access

no IPv6 | 113,5 GiB | DHCP: yes | VPN: no | W: 100% at Mordor | 172.16.1.101 | E: down | BAT 44,50% 01:25:42 | 0,13 | 2016-03-13 15:27:25



Nexpose Security Console :: Administration - Iceveasel

File Edit View History Bookmarks Tools Help

Nexpose Security Co... x

https://nexpose.s-m-s.pl:3780/admin/index.jsp

nexpose Create

Users
Create and manage user accounts and manage your password policy.

Asset Groups
Create dynamic or static asset groups and manage existing asset groups.

Exceptions and Overrides
Review requests to exclude vulnerabilities from reports and to override policy compliance results.

Calendar
View monthly calendar of all scheduled scans and reports.

Scan Options

ENGINES Create and manage available Scan Engines, and Scan Engine Pools.

SHARED CREDENTIALS Create and manage shared credentials for authenticated scans.

BLACKOUTS Create and manage global blackout settings.

HISTORY View complete scan history for this installation.

TEMPLATES Create and manage scan templates for controlling and tuning scans.

ROOT CERTIFICATES Manage root certificates used in scanning.

Discovery Options

NSX MANAGER Create and manage settings that give a Scan Engine direct access to an NSX network of virtual assets. Update the NSX OVF distribution.

CONNECTIONS Create and manage connections that allow the Security Console to discover assets dynamically.

Global and Console Settings

GLOBAL Manage global settings for selecting risk score strategies and excluding assets from scans.

CONSOLE Administer settings for the Security Console, including auto-update and logging settings.

no IPv6 | 113,5 GiB | DHCP: yes | VPN: no | W: 100% at Mondar | 172.16.1.101 | E: down | BAT 46,17% 01:40:19 0,39 | 2016-03-13 15:24:00

Aby edytować użytkowników przechodzimy do zakładki „manage” w dziale „Users”.



Nexpose - Wstępna konfiguracja

Nexpose Security Console :: Users - Iceveasel

File Edit View History Bookmarks Tools Help

Nexpose Security Co... x

https://nexpose.s-m-s.pl:3780/admin/users.jsp

nexpose Create

Users

<input checked="" type="checkbox"/>	Authenticator	User Name	Full Name	Email	Administrator	Last Logon	Password Expires	Disabled	Sites	Groups	Unlock	Edit	Delete
<input checked="" type="checkbox"/>	Nexpose user	nowy	Nowy User	nowy@domena.p l	Yes		N/A	No	0	0			
<input type="checkbox"/>	Nexpose user	pht	pht		Yes	3/13/2016 3:23 PM	N/A	No	0	0			

NEW USER DISABLE USERS ENABLE USERS

no IPv6 | 113,5 GiB | DHCP: yes | VPN: no | W: 100% at Morder | 172.16.1.101 | E: down | BAT 44,06% 01:37:21 | 0,42 | 2016-03-13 15:28:15

Aby wyłączyć użytkownika należy zaznaczyć go i kliknąć „Disable”.

I to na tyle ogólnej konfiguracji - na ciąg dalszy zapraszamy już niedługo!