

NetWatcher® Managed Detection & Response Service Installation Guide

What is NetWatcher?

NetWatcher is a Security-as-a-Service platform that enables customers to have a cost-effective 24 x 7 security service monitoring their networks for vulnerabilities and exploits. Many government and industry compliance requirements, and security best practices, outline the need for continuous monitoring, intrusion detection, active scanning, log monitoring, net-flow analysis, event management and endpoint integration. NetWatcher enables customers to immediately deploy these services and take advantage of a fully-staffed Security Operations Center (SOC). This means superior security that is easy to use, accurate and affordable.



Contents

| Connecting Hardware Sensor to NetWatcher Cloud | 3 |
|--|----|
| Setting up Network Intrusion Detection (NIDS) | 4 |
| Setting up SYSLOG Ingestion | 4 |
| Setting up Server / Desktop / Laptop LOGS | 6 |
| Setting Up Reoccurring Vulnerability Scans | 8 |
| Setup Reoccurring Reports | 10 |
| Setup Notifications | 11 |
| Connecting Virtual Sensor to NetWatcher Cloud – VSphere | 12 |
| Installing the Virtual Sensor on Other Virtual Machine Platforms | 19 |





Connecting Hardware Sensor to NetWatcher Cloud

- 1. The NetWatcher team should have sent you an Activate email that will allow you to create your Customer Portal account. If you didn't get this send a note to info@netwatcher.com and someone will assist you.
- 2. Ensure you are not blocking any of the following ports OUTBOUND. These ports are what the sensor uses to communicate back to the NetWatcher cloud.
 - TCP 22 => portal.netwatcher.com
 - TCP 8443 => p.netwatcher.com
 - UDP 443 => vpn.netwatcher.com
 - TCP 443 => vpn-tcp.netwatcher.com
 - TCP 443 => index.docker.io
 - TCP 443 => registry-1.docker.io
 - TCP 443 => public.update.core-os.net
 - TCP 80 to google.com => Used to test internet/DNS connectivity
- Connect one of the LAN ports on the sensors to the internet (doesn't matter which one) and let the sensor download its OS/Containers/Rulesets. This can take 20 min. The sensor light on the 'sensors' tab in the Customer Portal will go amber if the sensor sets itself up correctly.
- 4. If you need to setup a static IP address see this article.
- 5. Run Setup <u>https://portal.netwatcher.com/setup</u>



Setting up Network Intrusion Detection (NIDS)

6. Create a mirror of the port that the firewall is plugged into on the router/switch

Here is an example of setting up a mirror on a NetGear managed switch:

| Prosafe Plus Configuration Utility-GS105Ev2 | | | | | | - 🗆 × |
|---|--|--------------------|-----|----|------------------------|------------------------------|
| NETGEAR Connect with Innovation Network System VLAN Statue Maintenance Manipaire | QoS Help MultiCast Manag | ement | | | Select Lang English | GS105Ev2 uage: ↓▼ QUIT |
| Port Statistics *Mirroring Cable Tester | Port Mirroring Port Mirroring Confi Mirroring Source Port | guration Enable | · · | | | |
| | Port Destination Port | 01 x 03 | 02 | 03 | 04 | 05 |
| | | | | | | |
| | | | | | CANCEL | APPLY |
| Copyright @ 1996-2014 Netgear @ | | | | | | |

- 7. Connect the other LAN port on the sensor to the newly created mirror port.
- 8. Verify the sensor light turns green on the sensors tab in the Customer Portal

If you are setting up the SIEM for log aggregation this is accomplished in 2 parts (setting up hardware SYSLOGs like firewalls and setting up servers and desktop logs)

Setting up SYSLOG Ingestion

- Verify the device you want to monitor is on the supported device list found here.
- In the Customer Portal go to the "Sensors" tab and select the sensor that you want to receive the logs and choose the Actions | Log IPs option.

| 🕡 NetWatcher | Invite a friend and get one month free | Scott Suhy 🌲 Logout & |
|------------------------------------|---|---------------------------|
| 🖵 Dashboard 🛛 🗠 Reports 🔹 🌲 Alarms | $ \Xi $ Sensors $ \equiv $ EndPoints | d 💁 Support |
| My Sensors | | |
| Active or Not Sensor Name | Opened Alarms Service Installed | Groups 🔶 Actions |
| oe_lamer-oe 10.20.7.68 | 23 SYSLOG SCANNE | • |
| Display: 100 • | < 1 > | E Log IPs |
| Additional Services | | E Log Rules |
| S Enable Logs for all Sensors | ☑ Enable Scanning for | (2) Syslog Questionnaire |



11. Choose "Add new IP"

| 7 NetWatcher | Invite a friend and get one month free | Scott Suhy 🔺 Logout 🖙 |
|--|---|---------------------------|
| 🖵 Dashboard 🛛 🗠 Reports 🔹 🌲 Alarms | anced 💊 Support | |
| Log IPs | | + Add new IP |
| Total Log Assets: 17 Manual Log Assets: 4 NetAgent | Log Assets: 13 | |

12. Add the IP of the Device

| 🟹 Net | tWatcher | Invite a friend and get one month free | Scott Suhy A Logout & |
|-----------|-----------------------------|---|---------------------------|
| 🖵 Dashbo | oard 🛛 🗠 Reports 🔹 🌲 Alarms | ≅ Sensors 🛛 ☴ EndPoints 🛛 🎕 Advar | nced 🗠 Support |
| Edit allo | wed IP | | |
| Source IP | 10.20.20.1 | | |
| Sensor | oe_lanneroe | × | |
| ✓ Save | (Cancel | | |

13. Go back to the main page under the 'Sensors' tab and select Action | Syslog Questionnaire

| V NetWatcher | Invite a friend and get one month free | Scott Suhy 🔺 Logout 🛛 |
|---------------------------------|---|---|
| 🖵 Dashboard 🛛 🗠 Reports 🔹 🌲 Ala | ms 幸 Sensors ≡ EndPoints �\$ Advanced | 🇠 Support |
| My Sensors | | |
| Active or Not Sensor Name 🗢 II | ddress | Groups 🗢 Actions |
| • oe_Janner-oe 10 | 0.7.68 23 SCANNER | 0 |
| Display: 100 • | < 1 > | E Log IPs |
| Additional Services | | Syslog Questionnair |
| Enable Logs for all Sensors | ☑ Enable Scanning for all Sen | ISOTS |
| | | |



14. Select the device type that is sending the SYSLOG. If it is not on the list, choose 'Ask Question' and specify the device and the DevOps team will enable the ruleset manually.

| 🖵 Da | shboard 🗠 Reports 🔒 Alar | ms 🗦 Sensors | ≡ EndPoints | 🕫 Advanced | | 🐿 Support |
|------|--------------------------|------------------|-------------|------------|---|--------------|
| ЛуS | ensors > Syslog Question | naire for oe_lan | nneroe | | | |
| | Barracuda | | | | 0 | Ask question |
| | Cisco - All | | | | _ | |
| | Cisco - ASA | | | | | |
| | DHCPCD Server | | | | | |
| | dnsmasq (DHCP) | | | | | |
| | Fortinet | | | | | |
| | HP ProCurve | | | | | |
| | Juniper - All | | | | | |
| | Meraki | | | | | |
| | OpenVPN | | | | | |
| | Palo Alto | | | | | |
| | SonicWALL | | | | | |
| | WatchGuard | | | | | |

Setting up Server / Desktop / Laptop LOGS

15. Got to the 'Endpoints' tab and choose the green 'Download NetAgents' button. Remember that the NetAgent is free and can be run on any supported Windows or Ubuntu/Redhat Linux asset.

| 7 NetWatcher | | ta da | | | | () | cott Suhy | | |
|----------------------------------|---------------|---|----------|----------|----------|-----------|--------------------------|---|---------|
| 🖵 Dashboard 🔰 🗠 Reports | Download | d NetWat | cher® A | gent | | × | | 🛳 Support | |
| Net Agents Logs Net Agents | w 🖿 م | ndows EXE nux (Beta) | | at Wind | dows MSI | | ≛ Do | wnload NetAgent | |
| Available Modules Counts | | | - | - | - | | | | |
| ∀ Filters | | | | | | | | | |
| With selected: Actions * | | | | | | | | | |
| Asset 🗢 Hostname | IP address | иас | Events 🗢 | Alarms 🗢 | | | Last Checkin 🖨 | Modules | Actions |
| Scott's HP hp- 8570w | 10.20.1.39 c | 18:9d:67:d3:68:7b | 23840 | 0 | | | Less than a minute ago | HIDS Logs Sensor in the Cloud Systray | ~ |
| 🗌 🌰 Adam Work 🤅 desktop-51:54197 | 10.20.1.37 ! | 38:82:a8:98:3a:25 | 7906 | 0 | | | Less than a minute ago | HIDS Logs Sensor in the Cloud Systray | ~ |
| 🗌 🛎 Laurens old laptop-45alhóg | 10.18.0.191 3 | 0:52:cb:93:05:44 | (1513) | 0 | | | About 3 minute(s) ago | HIDS Logs Sensor in the Cloud Systray | ~ |
| 🗌 🌰 10.18.1.46-b bjerry-ponew | 10.19.31.2 | 00:ff:c3:39:b1:ae | 1659 | 0 | | | Less than a minute ago | HIDS Logs Sensor in the Cloud | ¥ |



16. Once the NetAgent has been deployed the asset will show up on the list (may take a few minutes). Select 'LOGS' and the following dialog box will appear—choose Action 'Install' for LOGS. Repeat for HIDS if you want to install the Host Intrusion Detection Logs as well.



17. The Dialog box will reflect a Pending Install and in a minute or so the Logs will begin to send to the sensor. If the sensor is not live, the Logs will go directly to the cloud over a secure VPN until the sensor goes live again.

| 0 | Scotts Dell | Undefined 10.20.4.35 | 90:e2 | :ba:2c:45:d8 | 69727 | 0 | 90 | 82 | About 18 | Hit Module is nov Sersor in the Court Systray | v waiting for 'i | nstall' × |
|---|----------------|--------------------------|-------------|--------------|---------|------------------|------------|------|-------------------------|---|------------------|-----------|
| 0 | 🌢 ubuntu-05d | Name | Version | OS | Pending | Status / Desired | Last Error | Acti | s) ago | HIDS Logs Sensor in the Cloud | * | |
| 0 | localhost-43 | Logs | | windows | INSTALL | | | |) ago | HIDS Logs Sensor in the Cloud | ~ | |
| | a osboxes-Tos | HIDS | | | | | | | to 3 | HIDS Logs Sensor in the Cloud | ~ | Fee |
| 0 | 🌢 ubuntu-71c | Sensor in the Cloud | | | | | | , |) ago | HIDS Logs Sensor in the Cloud | ~ | edback |
| | 🌢 osboxes-Defi | | | | | | | |) ago | HIDS Logs Sensor in the Cloud | ~ | |
| 0 | | win-gSem5da17 10.18.1.18 | D 00:0c | :29:01:22:0e | 2 | 0 | | | About 1 month(s) ago | HIDS Logs Sensor in the Cloud Systray | * | |
| 0 | a racerxs-mac | racerxs-mac 192.168.13 | 4.139 00:00 | 29:86:a9:71 | 0 | 0 | 100 | 100 | About 1 day(s) ago | Logs | * | |



Setting Up Reoccurring Vulnerability Scans

18. Got to the 'Advanced' tab (you need to have 'Intermediate' checked in your user profile to see the 'Advanced' tab) and choose the 'Scanning' button and then choose the 'Create Scan Job' button.

| V NetWatcher | Invite a friend and get one month free | Scott Suhy 🔺 Logout 🖙 |
|------------------------------------|---|---------------------------|
| 🖵 Dashboard 🛛 🗠 Reports 🔹 🌲 Alarms | $ \equiv $ Sensors $ \equiv $ EndPoints | 🗞 Support |
| Events Assets Scanning | Networks | |
| Vulnerability Scanner | | + Create Scan Job |

19. We want to setup 2 scans (Discovery daily and a Full and Fast on a Weekend)

| Step 1: Setup the Discovery scan. | 🕡 NetWa | tcher | get one n | iend and nonth free | Scott Suhy A Logout @ | |
|--|--|---|-------------------|---|---|--|
| Note how the 'full network scanning' checkbox is checked. This ensures we see every IP in the range provided. Don't generate a report from the Discovery scan as it is not | Create Scan | Assets Scanning | S 호 Sensors 를 En | dPoints 0 ° Advanced | Support | |
| necessary. | Job Name | Discovery (Reoccurring) | | | | |
| | Description | | | Only Network Vulnerability Ter information of the target syste | ts are used that provide the most possible m. No vulnerabilities are being detected. | |
| | | | 4 | | | |
| | Sensor | oe_lanneroe | | | | |
| | Credentials | No credentials | | | | |
| | Scan Config | Discovery | | discovery | | |
| | Full Network | Check | | | | |
| | Scanning Scan now | | | | | |
| | Schedule Method | First Time | 2017-06-22 19:00: | | | |
| | | Schedule Period: 1 | day(s) + | | | |
| | | Maximum Duration | hour(s) - | | | |
| | Active / Enabled Auto Generate Report Targets | nothing | | IP/CIDR | | |
| | Assets Netwo | ns | | TIPS & CIOPS List | | |
| | L m m | | | | | |
| | | orks efault network (oe_lanneroe) | | IP/CIDR + Please, | Add | |
| | | Subnet 192,168.0.0/16 (28 Assets) Subnet 172.16.0.0/12 (2 assets) Subnet 10.0.0.0/8 (1810 assets) Subnet fc00::/7 (0 assets) | | ₫ 10.20.1.0/24 × | Clear All | |



Step 2: Create the Full and Fast Scan

For this scan, you will not need to check the 'Full Network Scanning' because the Discovery scan already found all the assets. This will greatly shorten the time the "Full and Fast" scan runs. You also might want to generate a report and have it sent to an email address. To add credentials, go to <u>https://portal.netwatcher.com/account</u> and choose the 'credentials button'.

Note: Always schedule the "Discovery" scan at least 2 hours ahead of the "Full and Fast" scan so they don't overlap.

| 🗸 NetWa | tcher | get of | a friend and ne month free | Scott Suhy A Logout (+ |
|-----------------------------|--------------------------------------|--------------------|---|---|
| Dashboard | 🗠 Reports 🔰 🌲 Alar | ms 🛛 🖨 Sensors 📄 🗄 | EndPoints Of Advanced | 👟 Support |
| Evers | Atsets Samu | Networks | | |
| Create Scan | Job | | | |
| Job Name | Full and Fast (Reoccurring) | | Scan Config Description | |
| Description | | | Only Network Vulnerability Test system, Plugins are optimized in faise negative rate especially low | s are used that will not damage the target the best possible way to keep the potential x. |
| Sensor | oe_lanner-oe | * * | | |
| Credentials | No crodentials | | | |
| Scan Config | Full and fast | a. e | Full and Fas | it |
| Full Network Scanning | uncheck | | | |
| Scan now | | | | |
| Schedule Method | First Time | 2017-06-24 19:00: | | |
| | Schedule Period: Every | 1 week(s) + | | |
| | Maximum Duration | hour(s) + | | |
| Active / Enabled | e y | | | |
| Auto Generate Report | 🖻 🧹 Generate | | | |
| Upload To Custom Storage | | | | |
| Send To | Scott.Suhy@netwatcher.com | | Optional: Email | |
| Targets | | | | P/CIDR |
| Assets Networ | ks | | IPs & CIDRs List | |
| | orks efault network (oe_lanneroe) | ec) | IP/CIDR + Pisase, s | slect Add |
| | Subnet 172.16.0.0/12 (2 assets | 1 | ▲ 10.20.1.0/24 × | Chiar AP |



Setup Reoccurring Reports

20. Go to the 'Reports' tab in the Customer Portal and choose the 'Situational Awareness' report. This gives you an overview of the entire landscape. Create the report from the beginning of a month to the end of a month.

| 🗸 NetWatchei | r | ť | 1nvite c t get one | r friend and e month free | Q | Scott Suhy 🜲 Logout 🗭 |
|-----------------------|-------------|------------|----------------------------|-------------------------------------|-------|---------------------------|
| 🖵 Dashboard 🛛 🗠 Re | ports 💧 🌲 | Alarms 🗦 🗄 | Sensors 🛛 🚍 | EndPoints 🛛 🕫 Adva | anced | 🎕 Support |
| Create Report | our reports |] | | | | |
| 1 Туре | | | Includ | e columns | | 3 Period |
| Events | > | | | | | From: |
| Assets | > | | | | | 2017-07-01 |
| Alarms | > | | | | | То: |
| Tickets | > | | | | | 2017-07-31 |
| Situational Awareness | > | | | | | |
| Alarms With Comments | > | | | | | |
| | | | | | | |
| | | | | | | |
| ▶ Run | C Reoc | urring | 🐨 Save | | | |
| | | | | | | |

21. Choose where to send the report to (email address, but it will also store it on the portal for you to download in the future) and choose how often you want to receive the report.

| Dashboar | Add to Reoccuri | ing | | × | 💊 Suppo |
|-------------|-----------------------|----------------------|----------------|----------------------|---------|
| | General Information | | Include fields | | |
| Create Repo | Type Situational Aw | areness | | | riod |
| Events | Run as | Send To | | | |
| Assets | .pdf * | scott@netwatcher.com | | | |
| Alarms | Name | | Period | Starting At: | |
| Tickets | Situational Awareness | | Every Week | • 08/09/2017 2:17 Pt | |
| Situational | | | | | |
| Alarms With | | | | | |
| | | Done | | | |
| | | | | | |
| D Ru | un 🕓 Reocci | urring 😨 Save | | | |
| | | | | | |



Setup Notifications

22. Setup your notifications by choosing your name in the upper right corner of the screen.

| 🖌 NetWa | | 🕋 Int ge | Invite a friend and | | | Scott Suhy A Logout | |
|---------------|-----------|----------------|---------------------|-----------------------|---------------------|-------------------------|--|
| Dashboard | 🗠 Reports | 🌲 Alarms | 章 Sensors | ≡ E | ndPoints 🛛 🕫 Adva | anced | 🎕 Supp |
| Base Info | Searches | Credentials | | | | | |
| ontact Inforr | nation | ¢ | Change photo | 🗲 Edit | User Experience I | Profile | |
| First Name: | | | scot | t | O Basic 🗿 Ir | termedia | ate |
| Last Name: | | | suh | у | Shows more informat | ion and use | s technical terms. You should understand |
| Company: | | | Ocean's Edg | e | malware). | iu basic seci | ung principles (anterent kinds of |
| Email: | | scott.su | hy@gmail.cor | n | | | |
| Phone: | | +' | l (202) 557693 | 7 | Multi-factor Auth | enticatio | DISABLED |
| TimeZone: | (1 | UTC -04:00) Am | erica/New Yor | lew York 🗸 Enable | | | |
| | | ⊠ Em | ail | | D SMS | | O How often |
| Security | | Send Medium a | nd High 🛛 🔻 | | Send only High | ¥ | Send as soon as occurs 🔹 |
| Hygiene | | Don't sen | d v | | Don't send | Ŧ | Send as soon as occurs v |
| Scan | | Don't sen | d v | | Don't send | ¥ | Send as soon as occurs v |
| Policy | | Don't sen | d v | | Don't send | ¥ | Send as soon as occurs * |
| Saved Filters | | | Depends on f | ds on filter settings | | | Send as soon as occurs * |
| Score | | | Send score v | ia Email | | | Every Day * |
| Notifications | | | Send notifica | tions via | Email | | Send as soon as occurs * |
| | | | | | | | |
| Savo | | | | | | | |



Connecting Virtual Sensor to NetWatcher Cloud – VSphere

- 1. The NetWatcher team should have sent you an Activate email that will allow you to create your Customer Portal account. If you didn't get this send a note to info@netwatcher.com and someone will assist you.
- 2. Ensure you are not blocking any of the following ports OUTBOUND. These ports are what the sensor uses to communicate back to the NetWatcher cloud.
 - TCP 22 => portal.netwatcher.com
 - TCP 8443 => p.netwatcher.com
 - UDP 443 => vpn.netwatcher.com
 - TCP 443 => vpn-tcp.netwatcher.com
 - TCP 443 => index.docker.io
 - TCP 443 => registry-1.docker.io
 - TCP 443 => public.update.core-os.net
 - TCP 80 to google.com => Used to test internet/DNS connectivity
- 3. Log in to <u>https://portal.netwatcher.com/login</u> navigate to <u>https://portal.netwatcher.com/sensor/sensors</u>, click on your sensor, and press the download button next to the Virtual Machine. It will take a while to download as it's a large file. We use <u>http://www.7-zip.org</u> for compression and there is no password. There are two parts, extract the first one and it will continue into the second one. Unzip, then untar downloaded .xz file. Compare the SHA1 hash.



| V NetWatcher | nvite a friend and get one month free | 🜲 Logout 🕞 |
|----------------------|---|--------------|
| 🖵 Dashboard 🛛 🗠 Repo | orts 🔹 Alarms 🛛 🛱 Sensors 📄 🗮 EndPoints 🛛 🏟 Advanced | 🚳 Support |
| Sensors Logs | rtual00 | |
| Sensor Details | | [Hide] |
| Sensor Id: | 12a276d1-2c9f-43b6-93ea-26faeeb18e1d | |
| Name: | oe-virtual00 | |
| Date: | Dec-28-15 | |
| Local IP: | 10.20.1.11 | |
| Local DNS: | s43b693ea26faeeb18e1d.s.n-w.io | |
| Disk Usage: | Used: 1.1GiB, Free: 90.1GiB, Total: 94.6GiB, Percent Used: 1.1% | |
| Groups: | [Edit] | |
| One Time Password: | Get one-time password | |
| Virtual Machine: | Download [Built: Jun-26-17] | |
| Filename: | NetWatcher-12a276d1-2c9f-43b6-93ea-26faeeb18e1d.tar.xz | |
| Timestamp: | 2017-06-26 16:28:57 | |
| SHA1 Hash | 8a7b6111c445393af39ebc6eda23239c7eb167a4 | |
| Size | 602.17 MiB | |

 Understand your current VM architecture and map out how you will setup your sensor VM. Here is a typical setup:



5. Create a mirror of the firewall traffic for the Network Intrusion Detection (NIDS)

Example on a Cisco device: See https://learningnetwork.cisco.com/docs/DOC-26018



Identify Source port for SPAN

#show run int Gi1/0/24

Building configuration... Current configuration : 92 bytes interface GigabitEthernet1/0/24 description Trunk to Internet Firewall switchport mode trunk end

Identify Destination port for SPAN

#show run int Gi1/0/18

Building configuration... Current configuration : 86 bytes interface GigabitEthernet1/0/18 description Link to vm2 vmnic1 switchport mode trunk switchport nonegotiate end

Configure SPAN:

#monitor session 2 source interface Gi1/0/24

#monitor session 2 destination interface Gi1/0/18

6. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port







 Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port--Create the SPAN Port to mirror all traffic. Set VLAN ID to 4095 (Step 3) to ensure proper handling of VLAN tags.

| Add Network Wizard | | | | Add Network Wizard | | |
|--|---|--|--------|---|--|--|
| Connection Type Networking hardware can be p | partitioned to accommodate each service that requires connectivity. | | | Virtual Machines - I Virtual machine | Network Access es reach networks through uplink adapters attached to vSphere standard switches. | |
| Center Ipe Liebon A Ages Corrector Setting Sorrow | Connection Trypes * Vitual RecIde Aid a lakeder derovet to handle vitual muchte network traffic. * Vitacent The Vitament (2019) stuck handles traffic for the following LSK services management. | : sphere vitation, BCSI, MFS, and host | | Unselec desired | Beter tables in global cached and handling the related by Beter tables in the relation of the relation by Beter tables in the relation of the relation by Beter tables in the relation of the | 4 (1A4 8) 66.022 (1A4 30) above) and select t (vmnic1 above). |
| | | - Back Newton | Canori | Help | 1 | ≤ Back Next ≥ Cancel |
| Heb | | S DRA MEALZ | | | | |
| Help | | | | Add Network Wizard | 1 | |
| Add Network Wizard Virtual Machines - Connection S Use network labels to identify it | kettings migration compatible connections common to two or more hosts. | | | Add Network Wizard Ready to Complete Verfy that al re | te nev and modified vigatere standard avitches are configured appropriately. | |
| Bit Add Network Wazed Virtual Machine - Connection 5 Use network bible to derive Anno 2 Connection - Sector Connection - Sector Virtual V | Instance Comparison common to two or more hosts. | | | Add Network Wizard Ready to Competent Verty that are Connection. Trade Readerstore and the Readerstore and the Readerstore and the Readerstore and the | I Re and modified righters standard switches are configured appropriately. Hot entranceling will include the following new and modified standard switches: Present. Site Target and the following the following includes and modified standard switches: Present. Site Target and the following the following includes and modified standard switches: Site Target and the following the following the following includes and modified standard switches: Present. Site Target and the following th | |
| Uto Add Network Ward Witail Nachine - Connection S to entropy the second second second second Connection 2 Second Seco | Heritys: Impacts connections common to two or more hosts. Information Informatio | "SPAN Target" | | Add Network Wizard Ready to Competence With the Arrow of | te te te terest and modified vighters standard settless are configured appropriately. In the characterized on the bibliouring new and modified standard settless: The standard settless are and modified standard settless: | |

8. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port--Enable Promiscuous Mode



| | en 39 | | Ø vSwitch0 Properties | | (include) X |
|----------------------|--|---|--|---|-------------|
| B B g new 1 Denny 19 | Notis and Claritors | and a sector (4) | Ports Network Adapters | | |
| # # # | | | Configuration Summary | vSphere Standard Switch Properties | |
| - A CE Local | and and address (SAL S.S.A. 1992)744 Terring States, Taxono, Terring States, Terring States, Terring, Terring States, Terring, Ter | 1 | 왕 vSwitch 120 Ports | Number of Ports: 120 | |
| a major an | Perform New Signer Studen Lett Spher Statute Lett | 1 | SPAN Target Virtual Machine Port Gro | I do once of Properties | |
| | Property Relatives | tates addatating, manage | | MUNITED FORES | |
| | Nexuel Sanded Seith: rSeith Manuel, Hyperbil. | | | | |
| | Stringe Adjuters P. String Target 2, 4 - 4 - 4 - 4 - 1000 Full IP | | | Default Policies | |
| | Abacat Settaga | | | Security | |
| | From Research | | | Promiscuous Mode: Reject | |
| | Lamed holizes | | | MAC Address Changes: Accept | |
| | The Contraction DNG and Rooting | | | Terffe theolog | |
| | Automotive language | | | Average Bapfwith: | |
| | Week Review Station/Shido | | | Peak Bandwith: - | |
| | Security Inde | 1 | | Bunt See: | |
| | Hard Cardio Cardiocation Science Researce Receiption | | | Failover and Load | |
| | Apert VM Settings | | | Balancing | |
| | | | | Load baarong. Port ID Network Eaking Detection: Link status only | |
| | | | | Notify Switches: Yes | |
| | | | | Falback: Yes | |
| | Select Properties, Select vSwitch | 1 | Select Edit | Active Adapters: vmnk1 | |
| | | and the second se | | Standby Adapters: None | |
| | | | | Unused Adapters: None | |
| | | | | | |
| | | | | | |
| | A | | Add Edt Remove | 5 | |
| Bergent Looks | | Ners Teple Description - Test | | | |
| Name / Target | But a Detait Maker to contractional Reported Start - Start Time Compiled Time | | | | Close Help |
| | | | | | |
| | | | | | |
| VSwitch0 Prope | ties | | VSwitch0 Properties | | |
| General Security | Traffic Shaping NIC Teaming | 1 | General Security Traffic Shabing NIC Tea | imina | 1 |
| Policy Exception | ins | | Policy Exceptions | | |
| Promiscuou | s Mode: Reject | * | Promiscuous Mode: | Accept. | |
| MAC Addrer | s Changes: Accept | - | MAC Address Changes: | Accept | |
| | | - | Forged Transmits: | Accept | T |
| Forged Tran | ismits: Accept | and the second se | | | |
| Forged Tra | smits: Accept | | | | - |
| Porged Tra | ismits: Accept | | | | |
| Forged Tra | Ismits: Accept | | | | |
| Forged Tra | sents: Accept | | | | |
| Forged Tra | swritts: Accept | | | | |
| Forged Tra | smits: Accept | | | | |
| Forged Tra | eventes: Accept | | Enable Promiscuou | s Mode | |
| Forged Tra | ennes Accept | | Enable Promiscuou | s Mode | |
| Forged Tra | ennes: Accept | | Enable Promiscuou | s Mode | |
| Forged Tra | ennes: Accept | | Enable Promiscuou | s Mode | |
| Porged Tra St | elect Security Tab | | Enable Promiscuou | s Mode | |
| Forged Tra | ennes Accept | | Enable Promiscuou | s Mode | |
| Porged Tra St | elect Security Tab | | Enable Promiscuou | s Mode | м |
| Forged Tra | elect Security Tab | | Enable Promiscuou | s Mode | м |
| Forged Tra St | ennes: Accept | | Enable Promiscuou | s Mode | |
| Forged Tra | elect Security Tab | | Enable Promiscuou | s Mode | м |
| Forged fra | elect Security Tab | | Enable Promiscuou | s Mode | |

9. Import NetWatcher Sensor VM

| In the second provide th | NAware vCenter Converter Standalone | | Conversion | | |
|---|---|------------------|-----------------------------|--|----------------|
| A statistic of a statistic statisti statistic statisti statistic statistic statistic statistic sta | De yee lak American Bo | | Source Surtem | | |
| In the should look like this: | Sources gamer (a congre name) of | | Select the source sy | ystem you want to convert | |
| Click Convert machine: • Select source type: VMWare Workstation or other VMware virtual machine • Browse to and select .vmx file among your downloaded files • Browse to and select .vmx file among your downloaded files • Uncertainty system • The second select .vmx file among your downloaded files • Browse to and select .vmx file among your downloaded files • Contrast of the second with a machine file: Beld MetWacher - OUF wr • Destination .vm. • Destination . | Tod ID Joh ID Source Dedisation Statis Stat Time Forfilme | | | | |
| Click Convert machine: • Select Source type: VMWare Workstation or other VMware witual machine • Browse to and select .umx file among your downloaded files • Browse to and select .umx file among your downloaded files • Convert • A convert in the source statul machine file: statule machine file: statule adding or mage • Convert • A convert in the source statul machine or mage • A convert • A conv | | | Source System | - Source: none Destination: none | |
| Select source type: VMWare Workstation or other VMware virtual machine Browse to and select vmx file among your downloaded files Went VMare Morkstation or other VMware Virtual machine Browse to and select vmx file among your downloaded files Went VMare Morkstation virtual machine Went VMare Morkstation virtual machine Went VMare Vortual virtual machine Went Virtual virtual virtual machine Went Virtual virtual virtual virtual machine Went Virtual virtual virtual machine Went Virtual virtual | Click Convert machine: | | Destination System | | |
| Select source type: Vivware workstation or other Vivware virware type: Vivware virware vi | | A | Options | Select source type: VMware Workstation or other VMware virtual machine | <u> </u> |
| virtual machine Browse to and select .umx file among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the among your downloaded files Wene to the extent of the | Select source type: Viviware workstation or other Vivi | iware | Summary | Convert a virtual machine from VMware Workstation, VMware Fusion or other VMware product. | Player, VMware |
| Browse to and select .vmx file among your downloaded files Browse to and select .vmx file among your downloaded files Wenne Water Concerte Security Wenne Water and the met is the second with and the file is downloaded files Wenne Water and the met is the second with and the file is downloaded files Wenne Water and the met is the second with and the file is downloaded files Wenne Water and the met is the second with and the file is downloaded files Wenne Water and the met is the second with and the file is downloaded files Wenne Water and the met is the second with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded files Wether Details for Methade with and the file is downloaded with and the file is downloaded with and the file is downloaded with and the file is a wet with and the file is downloaded with and the file is a wet with and the file is a wet with and the file is a wet with and the file is downloaded with and the file is a wet with and the file is a wet with and the file is downloaded with and the | virtual machine | | | Total a such transfer product | |
| Browse to and select .vmx file among your downloaded files Browse to and select .vmx file among your downloaded files What is not the individual in the order is the of the select here to the order is the of the select here to the individual in the order is the orde | | 1.01 | | Browse for source virtual machine or image | |
| A constraint of the second | Browse to and select .vmx file among your downloade | ed files | | Virtual machine file: 8e1d\NetWatcher - Virtual\NetWatcher - OVF.vmx * | Browse |
| A constraint of the should look like this: It should look like this: | | | | Many service details | |
| How the function of the second secon | | | | view source getais | |
| Ad it should look like this: It is should look like this: It is should look like this: | Welcome to VMware vCenter Converter Standalone | | | | |
| A constraint of the second dispersion of th | Where vCenter Converter Standalone allows you to take one of a vanety of machines and convert this a new Offense altrud machines. The machines are used converting of the second machines are second machines. | | | | |
| d it should look like this: It should look like this: It should look like this: Bit should look like this: Source disk/outions: look: It should look like this: Source disk/outions: look: Source disk/outions: look: Source disk/outions: Source disk/outions: Source disk/outions: Source disk/oution: | Constant - The shall exclude a | | | | |
| Provide the second of the seco | Machine - VMware versal machines (vmu) | | | | |
| e. We want water of the second second | - Virtual Constrained Backup (, Virk) - Mereark Withial PC or Virtual Yerver virtual machines (, vinc) | | | | |
| Image: Strate of the strat | - Agreen Time Image Bokup (3k2) | | | | |
| Image: Instrument 3 Image: I | - StorageCraft ShadowStor (.spr) - Paralels Vitualization Products (.pvs) | | | | |
| 3 I dit should look like this: Machine yerse in Koware is soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the provide of the soor is a soor without before the soor is a soor without before the provide of the soor is a soor with a soor is a soor with a soor is a soor without before the soor is a soor with a soor is a soor is a soor with a soor is a soor is a soor with a soor is a soor with a soor is a soor is a soor is a soor with a soor is a soor is a soor with a soor is a soor is a soor with a soor is a soor is a soor with a soor is a soor with a soor is a soor is a soor is a soor is a soor with a soor is a soo | - Hyper-V vitual machines | | | | |
| 3 Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine Financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine financia it should look like this: Image: Matchine Uper UMinare desktop virtual machine financia it should look like this: Image: Matchine Uper UMinare Infrastructure virtual machine financia it should look like this: Image: Matchine Uper UMinare Infrastructure virtual machine financia it should look like this: Image: Matchine Uper UMinare Infrastructure virtual machine financia it should look like this: Image: Matchine Uper UMinare Infrastructure virtual machine financia it should look like like uniformatic (Valume 9) - 128 MB used / 128 MB ustal <ushoonna financia it should look like like uniformatic (Valume 9) - 128 MB used / 128 MB ustal <ushoonna financia it should look like like uniformatic (Valume 9) - 128 MB used / 128 MB ustal <ushoonna financia it should look like linke unifore financia it should like like like unifor</ushoonna </ushoonna </ushoonna | | | | | |
| 3 Machine type: Wew desktop virtual machine Firmware: BIOS Order 2 sol Tetal size: 500 GB Network: defenet0 Generation Source disk(s/viames) - 52.37 MB used / 128 MB total <td></td> <td> i</td> <td>Help Export dagr</td> <td>nostic logs Sext ></td> <td>Cancel</td> | | i | Help Export dagr | nostic logs Sext > | Cancel |
| Chick Next: Conversion | | | | | |
| 3 Image: NetWatcher - Out Image: Ne | Machine Details for NetWatcher - OVF | -X- | Conversion | | |
| Name: NetWorker NetWorker NetWorker NetWorker Ind it should look like this: To resting system: Chr (22 kb) Ind it should look like this: To resting system: Chr (22 kb) Ind it should look like this: To resting system: Chr (22 kb) Source disk/volumes is system: To resting system: Chr (22 kb) To resting system: Chr (22 kb) To resting system: Chr (22 kb) Source disk/volumes is system: To resting system: Chr (22 kb) To resting system: Chr (22 kb) To resting system: Chr (22 kb) Options Source disk/volumes is system: To resting system: Chr (22 kb) To resting system: Chr (22 kb) Options Source disk/volumes is system: To resting system: Chr (22 kb) To resting system: Chr (22 kb) Options Source disk/volumes is system: To resting system: Chr (22 kb) To resting system: Chr (22 kb) Options Click Next. Select Destination type: VMware Infrastructure virtual machine (Volume 3) - 168 used / 168 total (van | | | Destination System | | (4) |
| Machine type: Whare desktp vrtual machine Firmware: BIOS Operating system: Distribution type: Ind it should look like this: Source first operating is setter: Machine type: Whare desktp vrtual machine Sumce first operating system: Source first operating is them to the source in the source of the source in the source of the source in the source of the sou | Name: NetWatcher - OVE | A | Select a host for the new r | virtual machine | |
| Image: State Stat | Machine type: VMware desiton vitual machine | | | | |
| Operating system: 000-000 Operating system: 000-000 Operating system: 000-000 Operating system: 000-000 nd it should look like this: 500 GB Operating system: 000-000 Operating system: 000-000 Operating system: 000-000 RM: 4056 MB Operating system: 000-000 Operating system: 000-000 Operating system: 000-000 Operating system: 000-000-000 Sommy Where Inflatuture serve detail Sommy Operating system: 000-000 Operating system: 000-000-000 Sommy Where Inflatuture serve detail Sommy User serve detail Sommy Sommy Disk 1 <gpt> - 500 GB EH: +5YSTEM (Mame 1) - 6207 MB used / 128 MB total <atat> EA: +6WPT> Sommy User serve detail Sommy Sommy</atat></gpt> | Eirmurare: BIOS | | ource System Sou | arce: 🔁 1:\NetWatcher-12a\NetWatcher - OVF.vmx (Other (32-bt)) Destination: | |
| id it should look like this: Ioal size: 50 06 # Ivadia: Source disk/volumes log/set (4 socks * 1 cores) Rumber of vCPUs: 4 (4 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (4 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (4 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 4 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cores) Rumber of vCPUs: 5 (5 socks * 1 cor | Printware: Bios | D | Destination System | | |
| Ideal state: 500.08 Software VorWs: 4 (4 sodets *1 cores) Ideal is should look like this: 4 (a sodets *1 cores) Option RAM: 4006 HB Sermary Whater Initiation in the Water Initiation of the Water Initiation of the Water Initiation Sermary Whater Initiation Sermary Whater Initiation Sermary Whater Initiation Sermary Whater Initiation User anne: The Water Initiation in the Water Initiation Sermary User anne: The Water Initiation in the Water Initiation Sermary User anne: | Operating system: Other (32 bk) | Di | Pestination Virtual Mad | ct descriation gype: weiware initiastructure virtual machine | |
| d it should look like this: Number of vCVBs: {(1 socies 1 (cores) (| Total size: 500 GB | Di | Destination Location | Creates a new vestal machine for use on a velocite product. | |
| No. 1C. STICUTU FOOK TIKE CITIS. RAM:: 4056 HB Network: ethernet0 ethernet0 ethernet1 500 CC disks/columes Instructure server ocan Surce disks/columes Instructure 500 CC disks/columes Instructure Dist: + G07 - 500 GB 600 CC disks/columes Instructure (Winne 2) - 2 MB used / 12 MB total <unknown> Click Next. (Winne 3) - 128 MB used / 128 MB total <unknown> Click Next. (Winne 3) - 128 MB used / 128 MB total <unknown> Select Destination type: VMware Infrastructure virtual machine Server: This is your ESXi/vSphere cluster and login credentials. Server: This is your ESXi/vSphere cluster and login credentials.</unknown></unknown></unknown> | it chould look like this: | 0 | ummary | | |
| Network: ethernet0 ethernet1 = Source disks/volumes inyout = Dak 1 - G87 > 500 G8 = EF1-S7STM (Volume 1) - 62.97 MB used / 128 MB total <4h7> (Volume 3) - 66 used / 108 total <unknown> Click Next. Click Next. Select Destination type: VMware Infrastructure virtual machine Cyburne 0) - 128 MB used / 108 total <unknown> Select Destination type: VMware Infrastructure virtual machine Server: This is your ESXI/vSphere cluster and login credentials. Server: This is your ESXI/vSphere cluster and login credentials.</unknown></unknown> | RAM: 4096 MB | | , v | rimare initiasuscure server decails | |
| ethemetic Junce disk/volumes is suport: Disk 1 < GPT > 500 GB Disk 1 < GPT > 500 GB CH > System (Mame 1) - 6.9.7 MB used / 128 MB total < FAT > (Volume 2) - 2 MB used / 128 MB total < information | Network: ethernet0 | | S | erver: | |
| Source disks/volumes layout: Dak 1 GPT > 500 GB EFI-SYSTM (Volume 1) - 62.97 MB used / 128 MB total <47X> (Volume 3) - 1 GB used / 108 total <unknown> (Volume 4) - 1 GB used / 108 total <unknown> (Volume 4) - 1 GB used / 108 total <unknown> (Volume 5) - 128 MB used / 108 total <unknown> (Volume 6) - 128 MB total <unknown> (Volume 6) - 4MB total <unknown> (Volu</unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown> | ethemet1 | | U | Jser name: m | |
| Dok: 1 < GPT > - 500 GB EFI-SYSTEM (Volume 1) - 62.97 MB used / 128 MB total <fat> (Volume 2) - 2 MB used / 2 MB total <unknown> (Volume 4) - 16 B used / 106 total <unknown> (Volume 6) - 128 MB total <unknown> (Volume 6) - 4MB used / 148 MB total <unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></fat> | Source disks/volumes layout: | | P | Password: | |
| EFI-SYSTEM (Volume 1) - 62.97 MB used / 128 MB total <fm7> (Volume 3) - 16 Bused / 2 MB total Click Next. CVolume 3) - 16 Bused / 16 Butal Select Destination type: VMWare Infrastructure virtual machine Select Destination type: VMWare Infrastructure virtual machine Server: This is your ESXI/vSphere cluster and login credentials.</fm7> | Disk 1 <gpt> - 500 GB</gpt> | | | | |
| (Valume 2) - 2 HB used / 2 HB tetal <uknown> Click Next. (Valume 3) - 1 GB used / 1 GB tetal <uknown> Select Destination type: VMware Infrastructure virtual machine (Valume 3) - 1 GB used / 1 GB tetal <uknown> Select Destination type: VMware Infrastructure virtual machine (Valume 3) - 1 GB used / 1 GB tetal <uknown> Server: This is your ESXi/vSphere cluster and login credentials.</uknown></uknown></uknown></uknown> | EFI-SYSTEM (Volume 1) - 62.97 MB used / 128 MB to | otal <fat></fat> | | | |
| (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 GB total (Volume 3) - 1 GB used / 1 | (Volume 2) - 2 MB used / 2 MB total <unknown></unknown> | | Click Next. | | |
| Channe 9) - 120 MB used / 166 total <unknown> Channe 9) - 120 MB used / 166 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used / 418 total <unknown> Channe 9) - 418 MB used /</unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown></unknown> | (Volume 3) = 1 GR used / 1 GP total customers | | Select Dect | ination type: VMware Infrastructure virtual | machine |
| (Volume 5) - 1 of used / 1 do Net al Autonomic (Volume 5) - 1 de Net ad / 128 Net ad Autonomic (Volume 6) - 64 NE used / 64 NE total Autonomic | (Volume 4) - 1 GB used / 1 GB total < minimum | | Select Dest | ination type. Viviware initiastructure virtual | machine |
| (volume 5) - Las no uses / Las | (volume 4) - 1 GB used / 1 GB total <unknown></unknown> | | Server: Thi | is is your ESXi/vSphere cluster and login cred | dentials. |
| (Volume b) - 64 MB used / 64 MB total <unknown></unknown> | (Volume 5) ~ 128 MB used / 128 MB total <unknown></unknown> | · | | , | |
| | | | | | |
| (Volume 7) - 497.68 GB used / 497.68 GB total <unknown> *</unknown> | (Volume 6) - 64 MB used / 64 MB total <unknown></unknown> | | | | |

10. Import NetWatcher Sensor VM





11. Import NetWatcher Sensor VM

| Conversion | | Nhware vCenter Converter Standalone | × |
|--|--|---|------------|
| - | | Ele Vew Task Administration Help | |
| Summary | | 🕸 Convert machine 🍈 Configure machine 🔾 | |
| Review the conversion parameters | | Vieg by: * Tasks Show: * Al tasks in * Recent tasks | |
| | | Task ID Job ID Source Destination Status Start time End time | |
| Submitting job | | 19°1 1 WetWatche voerfet.svr 1% 12/30/2015 Estmated time remaining: 1 hours | |
| Destination System Destination Virtual Mach Source system information | ation | | |
| Options Could of the termination of termi | ENetWatcher-12a276d1-2c9f-43b6- None | | |
| Network throttling: | None | 🔁 VMware vCenter Converter Standalone | |
| Destination system info | ormation | Be View Jask Administration Help | |
| Virtual machine name: | NetWatcher - OVF | 😵 Convert machine 💩 Configure machine 😡 | |
| Hardware version: | version 10 | Vegr by: * Tasks Show: * Al tasks in * Recent tasks | |
| Connected as: | mckava | Task ID Job ID Source Destination Status Start time End time | |
| VM folder: | Defensative | SP 1 1 VetWatche vcenter.svr ✓ Completed 12/30/2015 12:19:59 PM | |
| Construction Construction Construction Construction Construction Construction Construction Construction Construction | Catobolis Default Default 4 (4 sockets * 1 cores) 4 dB Canneel de SPAN Target * | | |
| Hep Export diagnostic logs | < Back Ensn Cancel | Welcome to VMware vCenter Converter Standalone | |
| | | VMmere <center a="" a<br="" allows="" converter="" machines="" of="" one="" standalone="" take="" to="" variety="" you="">trio a new VMmere Vitali machine. The machine. The machine is you may convert include:</center> | id convert |
| | | Covert - Physical machines | |
| | | Machine - Whater vitual machines (vmx) | |
| | | - Vrware Considere associate (vrms) - Merosoft Vrtual PC er Vitual Server vitual machines (vrmc) | |
| Let it bui | ld. | - Synamic Ludvids Recovery Imag (xw2) - Arons Thur Image Roder, (x) - Arons Thur Image Roder, (x) - Arodek Virnauscon Products (xn) - Rodek Virnauscon Products (xn) - Rodek Virnauscon Products (xn) | |
| | | | |

12. Map NetWatcher Sensors Network Adapter 1 and Network Adapter 2





13. Open NetWatcher Sensor Console

| C C Margat, / conter second for | Clivphere clien D + O Cestificate erver O | gilance Login 🧭 «Sphere Web-Client 🛛 | | | | | | |
|--|--|--|----------------------------|---|----------------------------------|---|---|--|
| 🙀 🙋 Log In 🙋 HP BladeSystem Onbo | oard 🧭 HP OA - ProjT | | | | | | | |
| VmWord*VSphare Web C Voeter P 3 1 U 2 1 2 VGeter VGETER V | Ident Control Control Contro Contro Contro Contro Control Control Co | Read Opens | C nobyddial - i nig w | Recett Tasks Recett Tasks Al Running Failed Phone On straid machine Bit Mathiather - OVF Indialize percenting On | NetWatcher - OV File View VM | 'F on vm2.svr.oe.l | Click Actions->Open Console Verify IP Address | |
| Nindows FDrt - Adam | approximation on a what and approximations on called a generating system. Because every what matchine is an instantian machine a decision of every standard and events of the system of the system of the events of the system of the system of the system of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the events of the system of the system of the system of the system of the events of the system of the system of the system of the system of the events of the system of the system of the system of the system of the events of the system of th | Area for | | O Lood Poorlingse what machine Accordingse what machine According with the machine According with the machine Z March In Progress | | 0 8 0 0 0 | ₽ | |
| | In the second se | Austration Learn blood transfer agent version gradient learn about transfers Learn about transfers wer on the virtual | al machine | | | [156.186442] d [156.187465] d [158.984483] d [158.984483] d [158.994463] d [158.994463] d [158.994463] d [158.93563] d [159.833543] d [159.833543] d [159.833543] d [158.833543] d [158.833543] d [158.833543] d [158.83543] d [158.85436] d [158.8546] d [158.85466] d [158.85466] d [158.85466] d [| Invice withwelle?] left promiscious made inchest: port fivethwell??] antrand disable state inchest: port fivethwell??] antrand disable state invice withdis7784 entered premissions mode IP-06: OBBECONF(HTERUEUP): withdis7794; link because ready lockest?: port fivethalar7940 entered forwarding state obcets?: port fivethalar7940 entered forwarding state tockest?: port fivethalar7940 entered forwarding state lockest?: port fivethalar7940 entered forwarding state ent: fivetwards IDM-TMP device driver. 1.6 lockest?: port fivethalar7940 entered forwarding state entered forwarding state | |
| | | | | | | This is localmos SSH host key: Sh SSH host key: Sh SSH host key: Sh end 6777728: 18 end 6777728: 18 end 5554952: fe localhost login: | 11 - 551 - 552, 780 - 54 - 566 - 567 - 572, 783 - 783 | |

- 14. If you need to setup a static IP address see this article.
- 15. Login to the Customer Portal to Verify Sensor is Live (Sensor will turn amber if it can connect to the NetWatcher cloud; Sensor will turn green if it can also see the mirror/SPAN traffic)



Installing the Virtual Sensor on Other Virtual Machine Platforms

- For VMWare workstation (for testing only, not production) find details here
- For Hyper-V find details here

We hope you enjoy the NetWatcher service. We've designed the service to be useful for managers, help desk techs and for advanced security analysts. We've tried to make the User Interface (UI) intuitive and easy to use as well as powerful. If you have any questions don't hesitate to contact us at info@netwatcher.com

Follow us on Twitter @netwatcher.

https://netwatcher.com