Настройка аудита VMware ESXi и vCenter

VMware ESXi

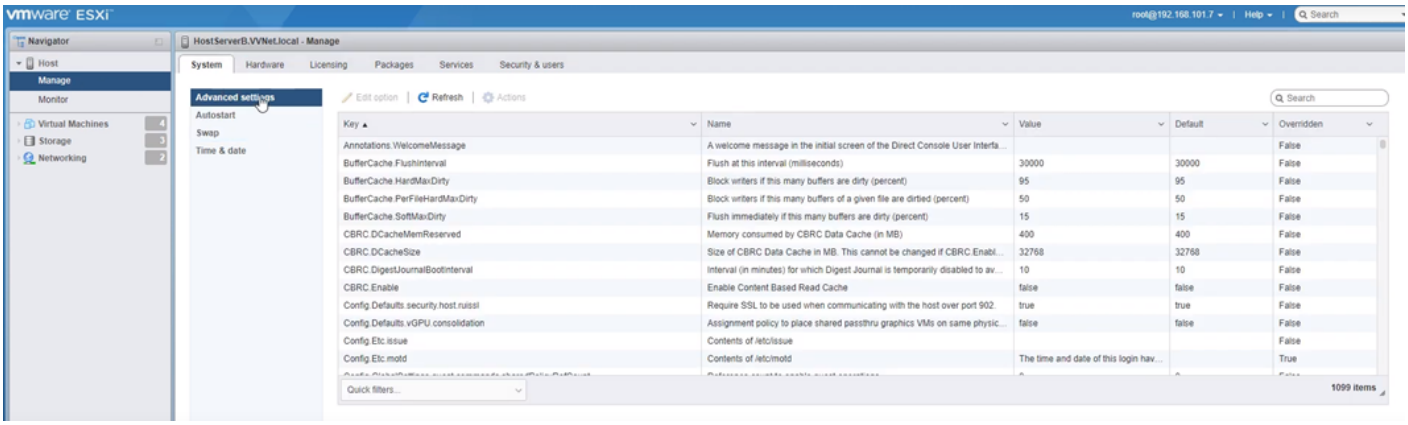
Через веб-интерфейс

????????? ???????????? ???????? ??????? ? ???????? ?????, ????????? ????????????? ? NTP-???????? (??????? ?? ????????, ??? ?? VMware ESXi ???????? ?????? ?? UTC).

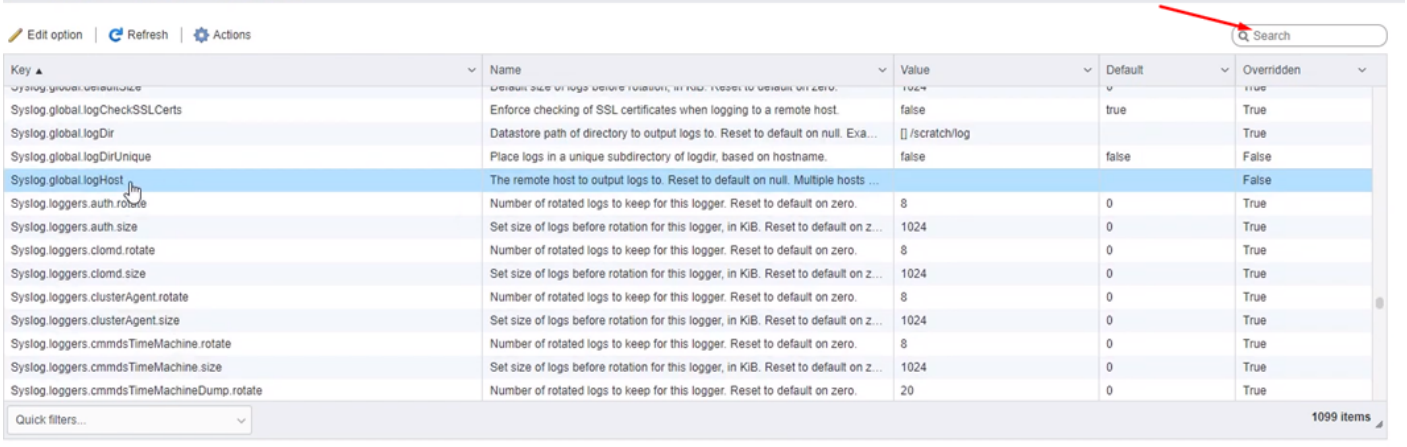
????????? ????????? ??????????? ???????????? ESXi-?????.

????? web-????????? ???????????? ? ESXi-????? ????????? ??????? ?????? root.

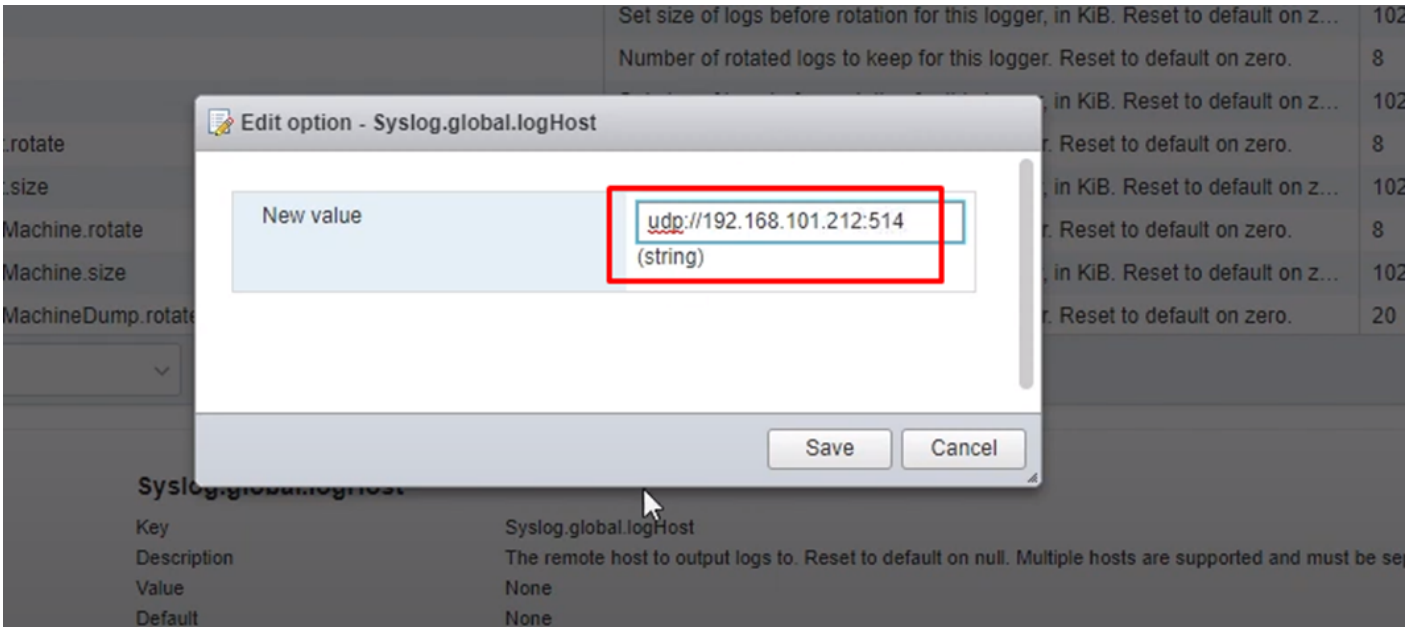
? ??????? ???? ? ??????? ????????? ?????????? ??????? Host ? ??????? ?? ????: **Host – Manage – Advanced Settings**.



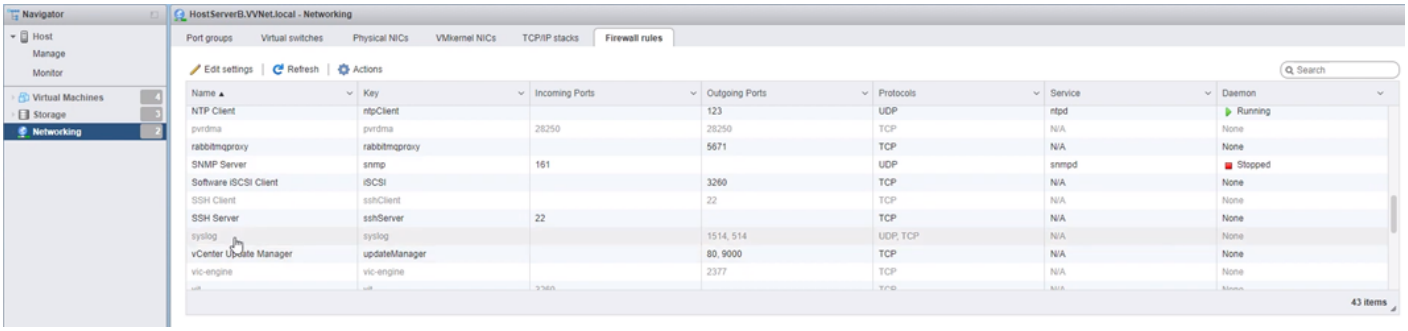
? ???? ?????? ??????? **Syslog.global.LogHost**, ??????? ???????? Syslog.global.LogHost ? ???????????????? ???.



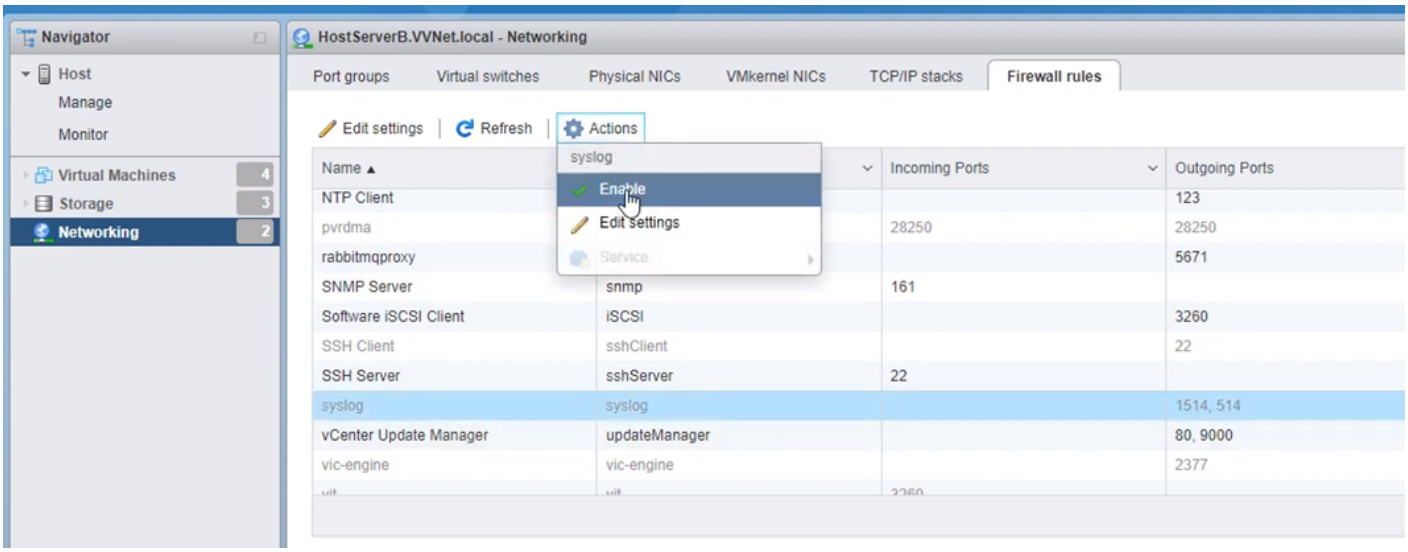
??????? ????????, ????? ? ???? ?????????? KUMA ? ??????? **Save**.



????? ????????? ?? ??????? **Networking – Firewall rules**.

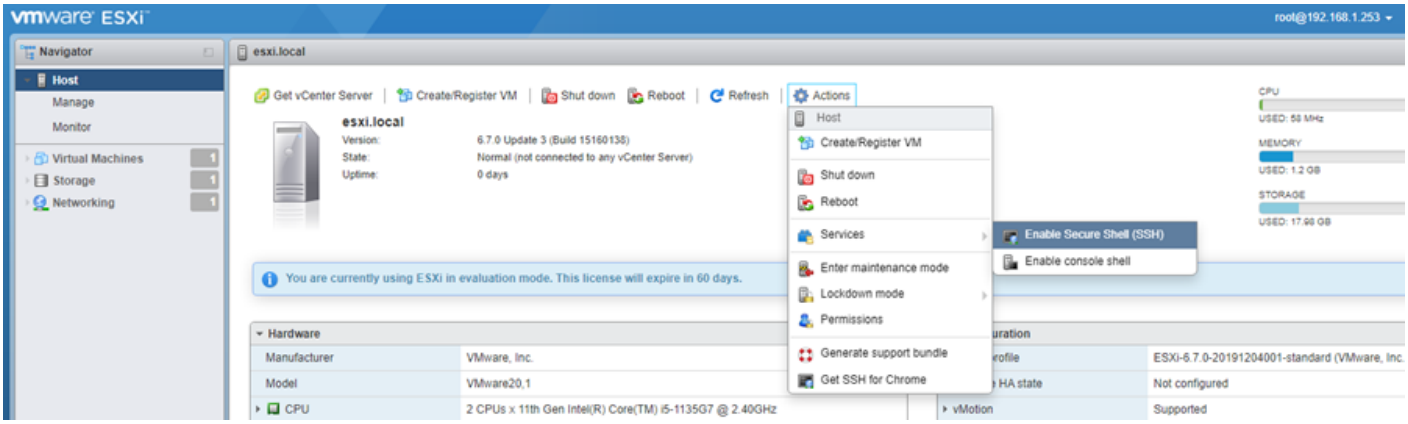


??????? ??????? syslog, ???????? ??? (????? ??????????????? ???????) ? ???????? ???, ????? ?? **Actions – Enable**.



Через SSH

????????? ?????? ????? ????????? ????? SSH. ???????? ?????? ?? SSH ?? ESXi-?????, ??????? ?? ???????: **Host – Actions – Services – Enable Secure Shell (SSH)**.



???????????? ? ESXi-????? ?? SSH ????????? ??????? ?????? root (???????? ????? Putty).

- ???????? ???????: `esxcli system syslog config set --loghost=udp://192.168.1.250:514` (???????????????? ??????????? ? syslog-???????, ip-????? ? ??????? ?? ???????? ?????????? ? ?????? ????????????? ??? ???????).
- ???????? ???????: `esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true` (????????? ???????????? ??????? ?????????? ??? syslog).
- ???????? ???????: `esxcli network firewall refresh` (?????????? ???????? ??????????? ?????? ESXi-?????).
- ???????? ???????: `esxcli system syslog config get` (???????? ???????? syslog-?????? ESXi-?????):

```
[root@esxi:~] esxcli system syslog config get
   Check Certificate Revocation: false
   Default Network Retry Timeout: 180
   Dropped Log File Rotation Size: 100
   Dropped Log File Rotations: 10
   Enforce SSLCertificates: true
   Local Log Output: /scratch/log
   Local Log Output Is Configured: false
   Local Log Output Is Persistent: true
   Local Logging Default Rotation Size: 1024
   Local Logging Default Rotations: 8
   Log To Unique Subdirectory: false
   Message Queue Drop Mark: 90
   Remote Host: udp://192.168.1.250:514
   Strict X509Compliance: false
```

- ??????? ???????: `esxcli system syslog reload` (???????????? syslog-?????? ESXi-?????).
- ?????????????? ?? ESXi-?????, ????? ??? web-????????? ??? ??????? ??????? ? ???????????????? ??????? ? **отключить доступ по SSH** (??????????: ???????? ????????????? VMware, ??????? ?? SSH ? ? ESXi-shell ????? ?????? ?? ????? ????????????? ? ????????? ?????).

(Опционально) ???? ?????????? ?????????? ??????? **Syslog на другой порт назначения**, ?????????? ???????? ??????? ??? ?? ESXi, ??? ????? ??????? ?? ???? ?? SSH.

???????? ???? (???????????? ???????????? Linux ???????) ?? ????????? ??????????, ???????? ??? ????? 5140 (??????? ???? syslogPort-5140.xml):

```
<!-- /etc/vmware/firewall/syslogPort-5140.xml -->
<!-- remote syslog configuration -->
<ConfigRoot>
  <service>
    <id>syslogPort-5140</id>
    <rule id='0000'>
      <direction>outbound</direction>
      <protocol>udp</protocol>
      <porttype>dst</porttype>
      <port>5140</port>
    </rule>

    <rule id='0001'>
      <direction>outbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>5140</port>
    </rule>

    <enabled>false</enabled>
    <required>false</required>
  </service>
</ConfigRoot>
```

??? ????????????? ????? ??????? ????????? ??????? ????, ? ?????????? ???:

- `cp syslogPort-5140.xml  /etc/vmware/firewall/`
- `esxcli network firewall unload`
- `esxcli network firewall load`

VMware vCenter

???????? snapshot ??? ????????? ????????? ??????????? vCenter.

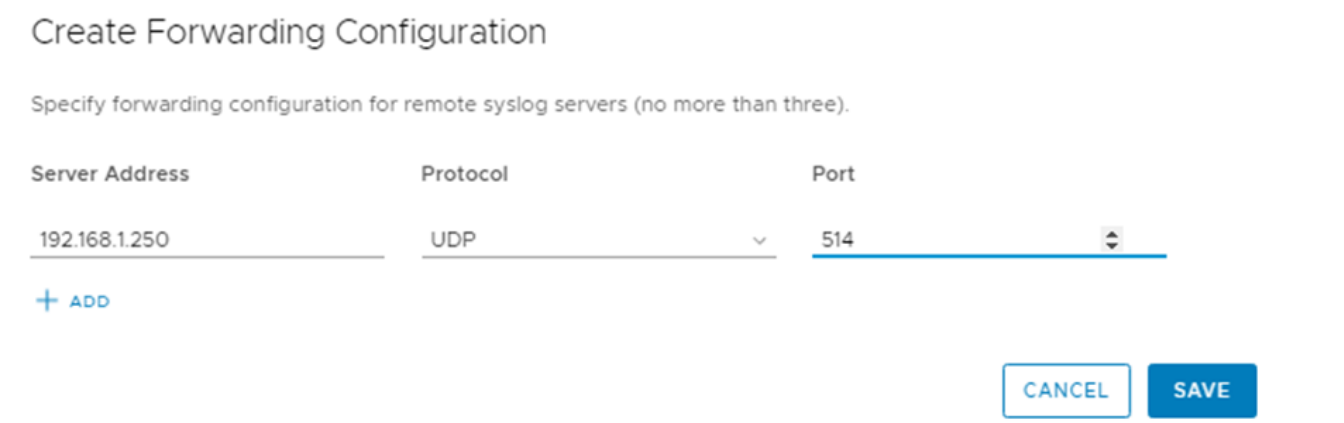
????? web-??????? ???????????? ? vCenter Server Appliance Management Inteface (VAMI) ????????? ???????????????? ??????? ?????? (????????, administrator@vsphere.local).

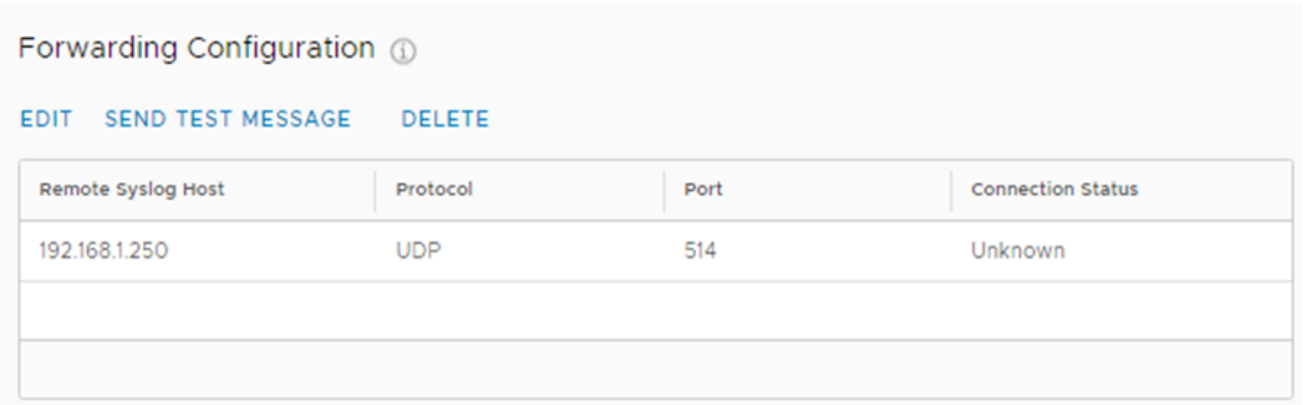
???????? ? web-????????: https://vcenter.test.local:5480 ? ?????? ???????????????? ??????? ?????? (??? vcenter.test.local ?? ???????? ?????????? ? ?????? ??? ???????).

????????? ? ???????????? ???????? ??????? ? ??????? Time (??????? ???? ?????? ? ???????? ???????, ? ??? ????????????? ? «???????» ????? ????????????? ???????? ?? ????????? ??????? ????????).

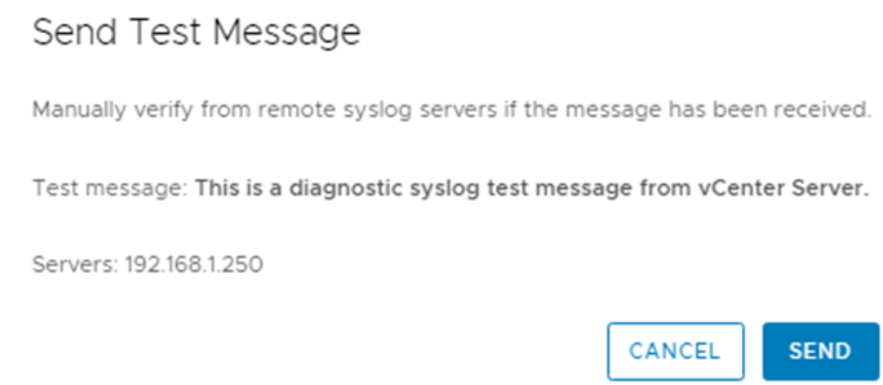


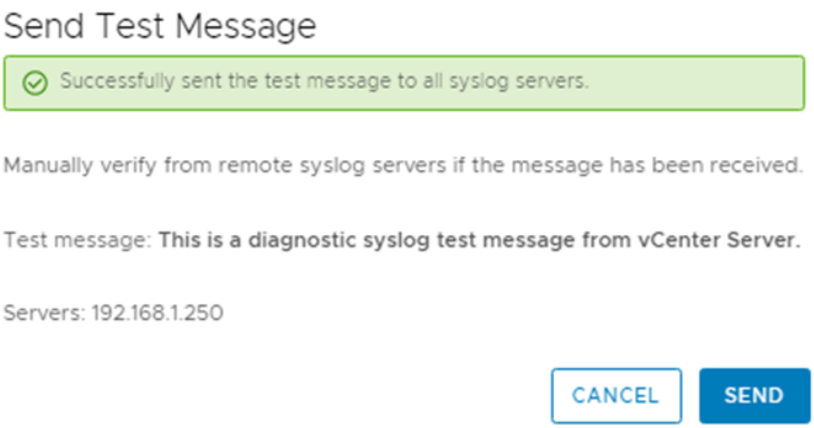
??????? ? ?????? **Syslog**, ????? ????????? Forwarding. ?????? ?????? **CONFIGURE**, ??????? ????????, ????? ? ???? ?????????? KUMA ? ??????? **Save**.





????????? ???????? ?????????:





Revision #2
Created 2023-11-14 09:50:12 UTC by Boris Rzr
Updated 2024-10-21 15:09:46 UTC by Koala