

Настройка аудита VMware ESXi и vCenter

VMware ESXi

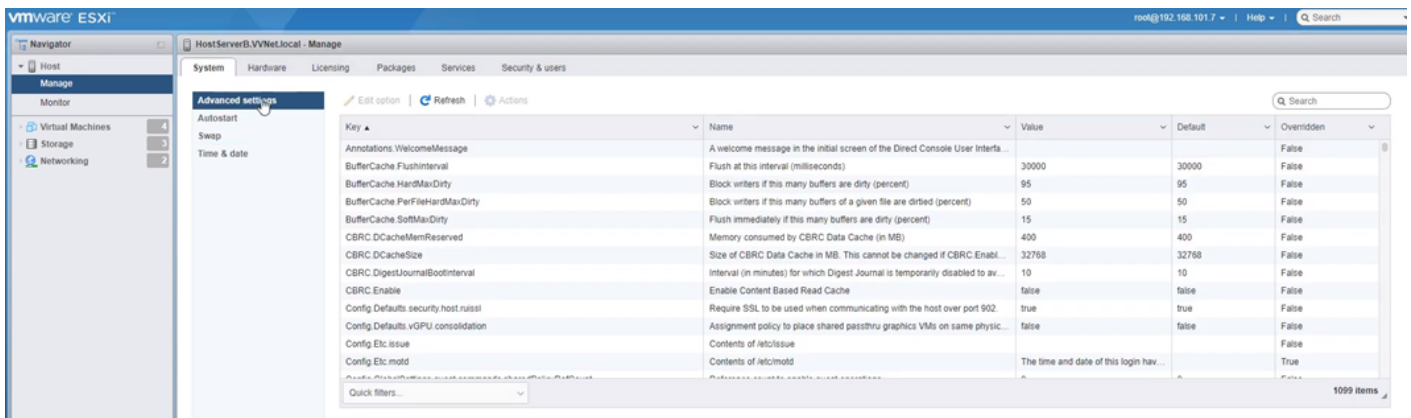
Через веб-интерфейс

Проверьте корректность настроек времени и часового пояса, проверить синхронизацию с NTP-сервером (принять во внимание, что ОС VMware ESXi работает только по UTC).

Выполнить резервное копирование конфигурации ESXi-хоста.

Через web-интерфейс подключиться к ESXi-хосту используя учетную запись root.

В главном меню в разделе навигации развернуть вкладку Host и перейти по пути: **Host - Manage - Advanced Settings**.



В окне поиска набрать **Syslog.global.LogHost**, выбрать параметр Syslog.global.LogHost и отредактировать его.

Edit option | Refresh | Actions

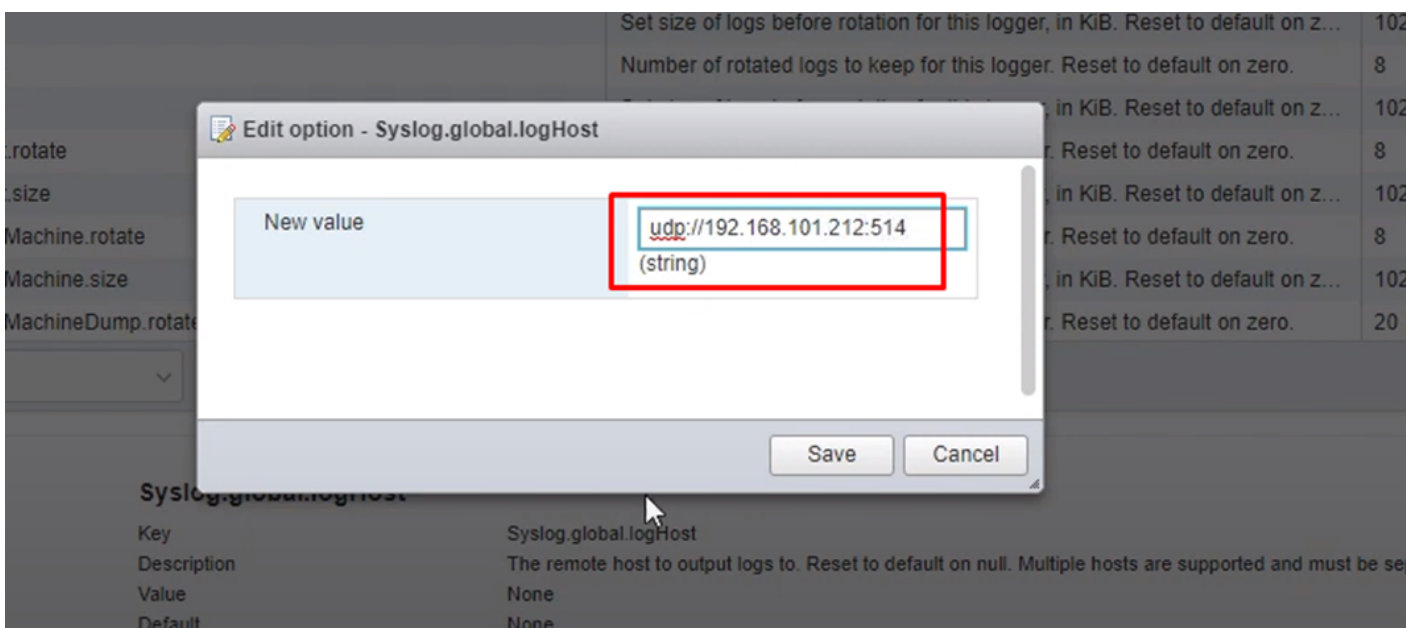
Search

Key	Name	Value	Default	Overridden
Syslog.global.verifySize	Default size of logs before rotation, in KiB. Reset to default on zero.	1024	true	True
Syslog.global.logCheckSSLCerts	Enforce checking of SSL certificates when logging to a remote host.	false	true	True
Syslog.global.logDir	Datastore path of directory to output logs to. Reset to default on null. Example: /scratch/log			True
Syslog.global.logDirUnique	Place logs in a unique subdirectory of logdir, based on hostname.	false	false	False
Syslog.global.logHost	The remote host to output logs to. Reset to default on null. Multiple hosts are supported and must be separated by a space.			False
Syslog.loggers.auth.rotate	Number of rotated logs to keep for this logger. Reset to default on zero.	8	0	True
Syslog.loggers.auth.size	Set size of logs before rotation for this logger, in KiB. Reset to default on zero.	1024	0	True
Syslog.loggers.clomd.rotate	Number of rotated logs to keep for this logger. Reset to default on zero.	8	0	True
Syslog.loggers.clomd.size	Set size of logs before rotation for this logger, in KiB. Reset to default on zero.	1024	0	True
Syslog.loggers.clusterAgent.rotate	Number of rotated logs to keep for this logger. Reset to default on zero.	8	0	True
Syslog.loggers.clusterAgent.size	Set size of logs before rotation for this logger, in KiB. Reset to default on zero.	1024	0	True
Syslog.loggers.cmmmsTimeMachine.rotate	Number of rotated logs to keep for this logger. Reset to default on zero.	8	0	True
Syslog.loggers.cmmmsTimeMachine.size	Set size of logs before rotation for this logger, in KiB. Reset to default on zero.	1024	0	True
Syslog.loggers.cmmmsTimeMachineDump.rotate	Number of rotated logs to keep for this logger. Reset to default on zero.	20	0	True

Quick filters...

1099 items

Укажите протокол, адрес и порт коллектора KUMA и нажмите **Save**.



Далее перейдите на вкладку **Networking - Firewall rules**.

HostServerB.VVNet.local - Networking

Port groups | Virtual switches | Physical NICs | VMkernel NICs | TCP/IP stacks | Firewall rules

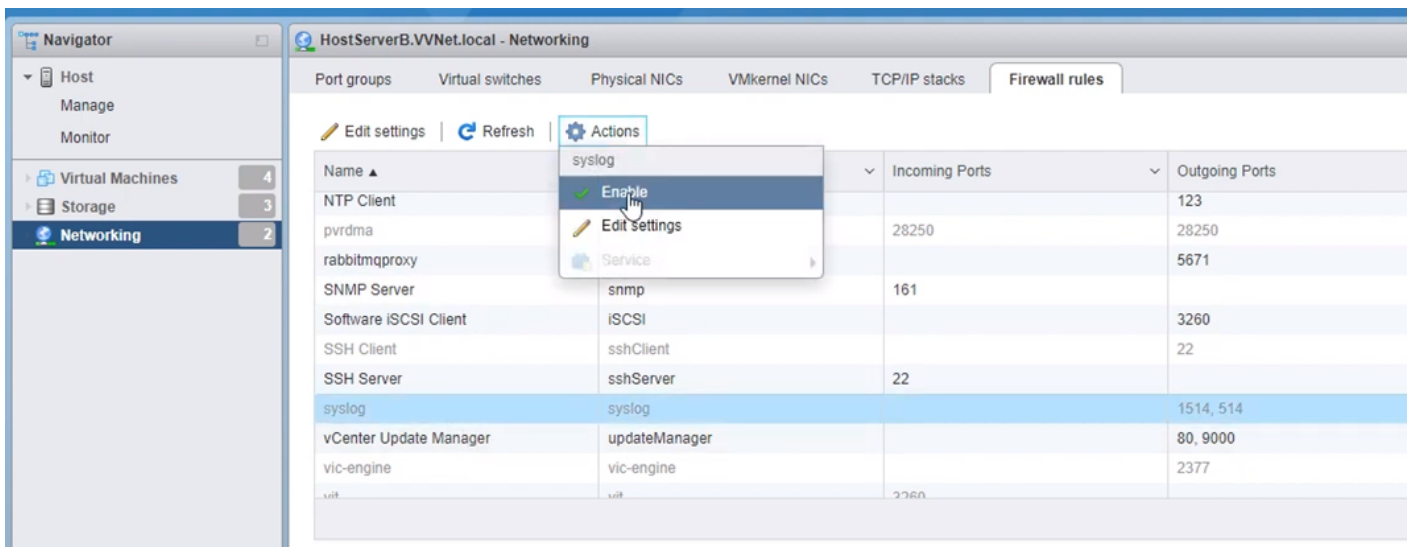
Edit settings | Refresh | Actions

Search

Name	Key	Incoming Ports	Outgoing Ports	Protocols	Service	Daemon
NTP Client	ntpClient		123	UDP	ntpd	Running
pvrdma	pvrdma	28250	28250	TCP	N/A	None
rabbitmqproxy	rabbitmqproxy		5671	TCP	N/A	None
SNMP Server	snmp	161		UDP	snmpd	Stopped
Software iSCSI Client	iSCSI		3260	TCP	N/A	None
SSH Client	sshClient		22	TCP	N/A	None
SSH Server	sshServer	22		TCP	N/A	None
syslog	syslog		1514, 514	UDP, TCP	N/A	None
vCenter Update Manager	updateManager		80, 9000	TCP	N/A	None
vic-engine	vic-engine		2377	TCP	N/A	None

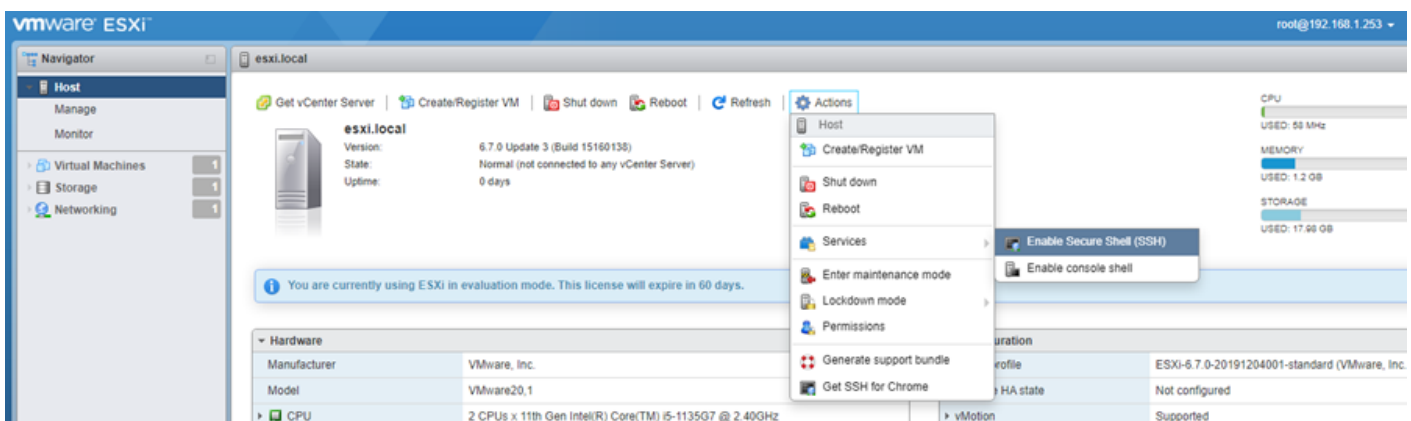
43 items

Найдите правило syslog, выделите его (можно воспользоваться поиском) и включите его, нажав на **Actions - Enable**.



Через SSH

Настройку аудита можно выполнить через SSH. Включить доступ по SSH на ESXi-хосте, перейти по пунктам: **Host - Actions - Services - Enable Secure Shell (SSH)**.



Подключитесь к ESXi-хосту по SSH используя учетную запись root (например через Putty).

- Наберите команду: `esxcli system syslog config set --loghost=udp://192.168.1.250:514` (конфигурирование подключения к syslog-серверу, ip-адрес в команде не является легитимным и указан исключительно для примера).
- Наберите команду: `esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true` (включение разрешающего правила фильтрации для syslog).
- Наберите команду: `esxcli network firewall refresh` (обновление настроек межсетевого экрана ESXi-хоста).
- Наберите команду: `esxcli system syslog config get` (проверка настроек syslog-службы ESXi-хоста):

```
[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
```

- Набрать команду: `esxcli system syslog reload` (перезагрузка syslog-службы ESXi-хоста).
- Авторизоваться на ESXi-хосте, через его web-интерфейс под учетной записью с административными правами и **отключить доступ по SSH** (примечание: Согласно рекомендациям VMware, доступы по SSH и к ESXi-shell нужны только во время диагностических и аварийных работ).

(Опционально) Если необходимо отправлять события **Syslog на другой порт назначения**, необходимо добавить правило для МЭ ESXi, для этого зайдите на хост по SSH.

Создайте файл (используются классические Linux команды) со следующим содержимым, например для порта 5140 (назовем файл 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>
```

Для использования этого правила выполните команды ниже, и активируйте его:

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

VMware vCenter

Сделайте snapshot или выполните резервное копирование vCenter.

Через web-браузер подключитесь к vCenter Server Appliance Management Interface (VAMI) используя административную учетную запись (например, administrator@vsphere.local).

Наберите в web-браузере: `https://vcenter.test.local:5480` и ввести административные учетные данные (имя `vcenter.test.local` не является легитимным и указан для примера).

Убедитесь в корректности настроек времени в разделе Time (часовой пояс указан в качестве примера, а тип синхронизации в «Филиале» будет индивидуально зависеть от указанных местных настроек).

Time zone	
Time zone	Europe/Samara
Time synchronization	
Mode	Host
Current appliance time	Wed 03-29-2023 11:42 AM +04

Перейти в раздел **Syslog**, чтобы настроить Forwarding. Нажать кнопку **CONFIGURE**, укажите протокол, адрес и порт коллектора KUMA и нажмите **Save**.

Create Forwarding Configuration

Specify forwarding configuration for remote syslog servers (no more than three).

Server Address	Protocol	Port
192.168.1.250	UDP	514

+ ADD

CANCEL

SAVE

Forwarding Configuration ⓘ

EDIT SEND TEST MESSAGE DELETE

Remote Syslog Host	Protocol	Port	Connection Status
192.168.1.250	UDP	514	Unknown

Отправьте тестовое сообщение:

Send Test Message

Manually verify from remote syslog servers if the message has been received.

Test message: This is a diagnostic syslog test message from vCenter Server.

Servers: 192.168.1.250

CANCEL

SEND

Send Test Message

✓ Successfully sent the test message to all syslog servers.

Manually verify from remote syslog servers if the message has been received.

Test message: This is a diagnostic syslog test message from vCenter Server.

Servers: 192.168.1.250

CANCEL

SEND

Revision #2

Created 14 November 2023 09:50:12 by Boris RZR

Updated 7 July 2024 08:48:09 by Koala