

ESXi

- [How to Identify disks and Datastore in VMware ESXi 5 / 6](#)
- [vSphere замена истекшего сертификата](#)

How to Identify disks and Datastore in VMware ESXi 5 / 6

There are a few reasons that will degrade the performance of virtual machines such as a disk I/O bottleneck, resource contention, misconfigurations and other problems.

When too many VMs compete for limited resources, results will inevitably suffer.

The effort it takes to solve the storage I/O bottleneck is a variety of ways, it may be from physical infrastructure choices to configuration changes.

The starting point for solving your I/O problems will be VM monitoring and establishing baseline performance.

From there, you can examine the IOPS read vs. write IOPS, network cards, and certain points which may contribute to the I/O bottlenecks.

With the right approach and the right technology, administrators can resolve the problems that caused the dismal performance of the infrastructure.

When performing troubleshooting with ESXi/ESX storage, use command line tools which require you to identify a specific disk or LUN connected to ESXi/ESX.

This article provides information on different ways to identify these disks. This can be part of troubleshooting, primarily due to the storage component of the virtual environment.

Display available command for esxcli storage :

```
~ # esxcli storage
Usage: esxcli storage {cmd} [cmd options]

Available Namespaces:
  core                VMware core storage commands.
  nfs                 Operations to create, manage, and remove Network Attached Storage
filesystems.
  nmp                 VMware Native Multipath Plugin (NMP). This is the VMware default
```

implementation of the Pluggable Storage Architecture.

san	I/O device management operations to the SAN devices on the system.
vflash	virtual flash Management Operations on the system.
vmfs	VMFS operations.
filesystem	Operations pertaining to filesystems, also known as datastores, on the ESX host.

Display available command for esxcli storage -> vmfs :

```
~ # esxcli storage vmfs
```

Usage: esxcli storage vmfs {cmd} [cmd options]

Available Namespaces:

snapshot	Manage VMFS snapshots.
extent	Manage VMFS extents.

Available Commands:

unmap	Reclaim the space by unmapping free blocks from VMFS Volume
upgrade	Upgrade a VMFS3 volume to VMFS5.

```
~ # esxcli storage vmfs extent
```

Usage: esxcli storage vmfs extent {cmd} [cmd options]

Available Commands:

list	List the VMFS extents available on the host.
------	--

List the VMFS extents available on the host :

```
~ # esxcli storage vmfs extent list
```

Volume Name	VMFS UUID	Extent Number	Device
Name			Partition
-----	-----	-----	-----
datastore1	52a0db3f-d87636dc-61bb-28924a2f1bc0	0	
t10.ATA_____VB0250EAVR_____		Z3TDY30B_____	3
datastore2	53f6103b-e2c46411-13e9-28924a2f1bc0	0	
t10.ATA_____WDC_WD1600AAJS2D00L7A0_____		WD2DWCAV36165769	1

```
~ # esxcli storage filesystem
```

Usage: esxcli storage filesystem {cmd} [cmd options]

Available Commands:

automount	Request mounting of known datastores not explicitly unmounted.
list	List the volumes available to the host. This includes VMFS, NAS, VFAT and UFS partitions.
mount	Connect to and mount an unmounted volume on the ESX host.
rescan	Issue a rescan operation to the VMkernel to have is scan storage devices for new mountable filesystems.
unmount	Disconnect and unmount and existing VMFS or NAS volume. This will not delete the configuration for the volume, but will remove the volume from the list of mounted volumes.

List the volumes available to the host. This includes VMFS, NAS and VFAT partitions :

```
~ # esxcli storage filesystem list
```

Mount Point	Volume Name			
UUID	Mounted	Type	Size	Free

/vmfs/volumes/52a0db3f-d87636dc-61bb-28924a2f1bc0	datastore1	52a0db3f-d87636dc-61bb-28924a2f1bc0	true	VMFS-5 244544700416 52979302400
/vmfs/volumes/53f6103b-e2c46411-13e9-28924a2f1bc0	datastore2	53f6103b-e2c46411-13e9-28924a2f1bc0	true	VMFS-5 159987531776 14871953408
/vmfs/volumes/556a99d3-4dc8997f-b819-28924a2f1bc0		556a99d3-4dc8997f-b819-28924a2f1bc0	true	vfat 4293591040 4255121408
/vmfs/volumes/4a052e7f-ed60f807-e327-66c4dcb34a59	Hypervisor1	4a052e7f-ed60f807-e327-66c4dcb34a59	true	vfat 261853184 96874496
/vmfs/volumes/25230d7e-4dcb47f9-390e-25a3db175fe7	Hypervisor2	25230d7e-4dcb47f9-390e-25a3db175fe7	true	vfat 261853184 96976896
/vmfs/volumes/2da668ef-40e5d96b-90bf-855ddb9c5547	Hypervisor3	2da668ef-40e5d96b-90bf-855ddb9c5547	true	vfat 299778048 96681984

```
~ # esxcli storage nmp
```

Usage: esxcli storage nmp {cmd} [cmd options]

Available Namespaces:

psp	Operations pertaining to the Path Selection Policy Plugins for the VMware Native Multipath Plugin.
satp	Operations pertaining to the Storage Array Type Plugins for the VMware Native Multipath Plugin.
device	Operations pertaining to the devices currently claimed by the VMware Native Multipath Plugin.

path Operations pertaining to the paths currently claimed by the VMware Native Multipath Plugin.

```
~ # esxcli storage nmp device
```

Usage: esxcli storage nmp device {cmd} [cmd options]

Available Commands:

list List the devices currently controlled by the VMware NMP Multipath Plugin and show the SATP and PSP information associated with that device.

set Allow setting of the Path Selection Policy (PSP) for the given device to one of the loaded policies on the system.

List the devices currently controlled by the VMware NMP Multipath Plugin and show the SATP and PSP information associated with that device :

```
~ # esxcli storage nmp device list
```

```
t10.ATA____VB0250EAVR_____Z3TDY30B_____
```

Device Display Name: Local ATA Disk

```
(t10.ATA____VB0250EAVR_____Z3TDY30B_____)
```

Storage Array Type: VMW_SATP_LOCAL

Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device configuration.

Path Selection Policy: VMW_PSP_FIXED

Path Selection Policy Device Config: {preferred=vmhba0:C0:T0:L0;current=vmhba0:C0:T0:L0}

Path Selection Policy Device Custom Config:

Working Paths: vmhba0:C0:T0:L0

Is Local SAS Device: false

Is USB: false

Is Boot USB Device: false

```
t10.ATA____WDC_WD1600AAJS2D00L7A0_____WD2DWCAV36165769
```

Device Display Name: Local ATA Disk

```
(t10.ATA____WDC_WD1600AAJS2D00L7A0_____WD2DWCAV36165769)
```

Storage Array Type: VMW_SATP_LOCAL

Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device configuration.

Path Selection Policy: VMW_PSP_FIXED

Path Selection Policy Device Config: {preferred=vmhba32:C0:T0:L0;current=vmhba32:C0:T0:L0}

Path Selection Policy Device Custom Config:

Working Paths: vmhba32:C0:T0:L0

Is Local SAS Device: false

Is USB: false

Is Boot USB Device: false

vSphere замена истекшего сертификата

vSphere замена истекшего сертификата vCenter Appliance

18 января 2022 [1](#) [Maxim Zhukov](#)

Недавно наш заказчик пришел с проблемой **потери управления виртуализированной инфраструктурой**.

356e0c6b-5b18-f0c2-3727-73a398523848?imagePreview=1

При попытке авторизации в консоль vSphere
An error occurred during authentication

```
Please configure certtool.cfg file with proper values before proceeding to next step.
Press Enter key to skip optional parameters or use Default value.
Enter proper value for 'Country' [Default value : US] : (Note: Value for Country should be
only 2 letters)
Enter proper value for 'Name' [Default value : CA] :
Enter proper value for 'Organization' [Default value : VMware] :
Enter proper value for 'OrgUnit' [Default value : VMware Engineering] :
Enter proper value for 'State' [Default value : California] :
Enter proper value for 'Locality' [Default value : Palo Alto] :
Enter proper value for 'IPAddress' [optional] :
Enter proper value for 'Email' [Default value : email@acme.com] :
Enter proper value for 'Hostname' [Enter valid Fully Qualified Domain Name(FQDN), For Example
: example.domain.com] :
Enter proper value for VMCA 'Name':
```

Ошибку следует диагностировать просмотром сертификата – который истек (видно из браузера).

При попытке входа в vCenter консоль (**Appliance Management**) для просмотра состояния сервисов

```
Exception in invoking authentication handler  
[SSL.CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:719)
```

Проблема в том, что при истекшем сертификате не попасть в консоль управления так как не может аутентифицировать, где по [процедуре](#) можно заменить сертификат из web- консоли.

7e776b5c-520a-e13c-40ac-3c1aa9dfddb3?imagePreview=1

Причину подтвердим просмотром трейса ошибки:

```
javax.net.ssl.SSLHandshakeException:  
com.vmware.vim.vmomi.client.exception.VlsiCertificateException:  
Server certificate chain is not trusted and thumbprint verification is not configured
```

Ошибки при истекшем сертификате будут вида

Что **такая-то служба** не может соединиться (так как **не устанавливается защищенное соединение с vCenter Appliance** из-за невалидного сертификата)

```
Authentication failed, Update Manager server could not be contacted.  
  
An unexpected error has occurred.
```

В том числе **не будет работать и служба Аутентификации vSphere**, а это, сами понимаете, «привет» управлению инфраструктурой и работе служб vSphere.

Что делать?

Нужно заменить истекший сертификат в vCenter Appliance. Но есть нюансы.

При отсутствии доступа в web-консоль **vCenter Appliance Management**

```
Exception in invoking authentication handler  
[SSL.CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:719)
```

Остается доступ через командную строку в виртуальную машину.

В ситуации с истекшим сертификатом работоспособность запущенных виртуальных машин не затронута, и можно зайти на узлы гипервизора ESXi и временно поуправлять вручную запуском и выключением виртуальных машин.

Собственно этот путь (**через подключения к ESXi**) с вызовом консоли машины с vCenter Appliance и потребуется проделать для замены истекшего сертификата, если на машине выключен **SSH** в целях безопасности.

Но где лежит сертификат и как его правильно заменить?

Оказывается, что для генерации сертификата vCenter Server Appliance имеет утилиту **Certificate Manager**.

Для начала подключитесь к vCenter через ssh или через консоль виртуальной машины с vCenter через гипервизор ESXi где она функционирует.

Если у Вас много хостов в инфраструктуре, возможно придется поискать последовательно подключаясь на каждый пока не отыщите свой запущенный vCenter.

1. Запустите `/usr/lib/vmware-vmca/bin/certificate-manager`

1. Если Вам приемлем Self-Signed Certificate и нужно быстро ВОССТАНОВИТЬ ДОСТУП

1. Выберите пункт **4 Regenerate a new VMCA Root Certificate and replace all certificates** и введите пароль для administrator@vsphere.local
2. Далее последовательно заполните поля с учетом того, что **Name, Hostname и VMCA должны соответствовать Primary Network Identifier PNID**.
3. Значение PNID можно посмотреть выполнив `/usr/lib/vmware-vmafd/bin/vmafd-cli get-pnid --server-name localhost`
- 4.
5. Нажмите Y (Yes) для продолжения.
6. В случае неактуального сертификата в веб-консоли vCenter перезагрузите vCenter.

2. Если Вы хотите валидный сертификат полученный через центр сертификации

1. В меню выберите пункт **1. Replace Machine SSL certificate with Custom Certificate** и введите пароль для administrator@vsphere.local
2. Укажите директорию, где будут помещены запросы на выпуск, например `/tmp/ssl/`
3. Далее последовательно заполните поля с учетом того, что **Name, Hostname и VMCA должны соответствовать Primary Network Identifier PNID**.
4. Значение PNID можно посмотреть выполнив `/usr/lib/vmware-vmafd/bin/vmafd-cli get-pnid --server-name localhost`

5. Country : Two uppercase letters only (Eg. US), the country where your company is located.
- Name : FQDN of the vCenter Server(This will be your Certificate Subject Alternate Name)
- Organization : Company Name
- OrgUnit : The name of your department within the organization.
- Example: "IT"
- State : The state/province where your company is located
- Locality : The city where your company is located.
- IPAddress : IP Address of vCenter Server, this field is Optional
- Email : Email Address
- Hostname : FQDN of vCenter Server(This field accepts multiple entries separated by comma.

6. Файл /tmp/ssl/vmca_issued_csr.csr передаем в центр сертификации для выпуска SSL сертификата.
7. Помещаем выпущенный сертификат на систему, например, в /tmp/ssl/ в отдельной сессии
8. Продолжаем импорт

Provide a valid custom certificate for Machine SSL.

File : /tmp/ssl/machine_name_ssl.cer

Provide a valid custom key for Machine SSL.

File : /tmp/ssl/machine_name_ssl.key

Provide the signing certificate of the Machine SSL certificate.

File : /tmp/ssl/Root64.cer

9. Нажмите Y (Yes) для продолжения.
10. В случае неактуального сертификата в веб-консоли vCenter перезагрузите vCenter.