POSITIVE TECHNOLOGIES

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107241 / МОСКВА / ЩЕЛКОВСКОЕ ЩОССЕ / Д.23А
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

CITRIX
XENSERVER FREE/ADVANCED 5.6

SECURITY HARDENING GUIDE

АВТОР: ЕРМАКОВ К.В.
EMAIL: KErmakov@ptsecurity.ru

ОГЛАВЛЕНИЕ

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1. ОБЩИЕ НАСТРОЙКИ СИСТЕМЫ

Данный раздел посвящен общим настройкам системы. Методология защиты аналогична таковой для стандартных серверов на базе ОС Linux.

1.1 Службы, запускаемые при старте Citrix XenServer

Требуется ограничить список служб, запускаемых при старте системы по умолчанию.

Настройка:

Для всех неиспользуемых служб выполните команду:

```
chkconfig <servicename> off
```

Здесь <servicename> — имя данной службы.

Для конкретного установленного сервера XenServer 5.6 результат выполнения команды должен иметь следующий вид (в зависимости от конфигурации сервера результирующая таблица может существенно отличаться):

```
chkconfig --list | grep 3:on

attach-static-vdis
crond
fcauthd
fe
iptables
lwsmd
management-interface
mpp
network
ntpd
perfmon
portmap
rawdevices
set-memory-target
snapwatchd
squeezed
sshd
syslog
unplug-vcpus
v6d
vhostmd
xapi
xapi-domains
xe-linux-distribution
xen-domain-uuid
xenservices
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1.2 Настройка синхронизации времени

Для корректной работы узлов XenServer как индивидуально, так и в режиме «pool» необходима синхронизация времени. Можно использовать как собственный NTP сервер, так и предоставляемые настройкой по умолчанию.

Настройка:

Добавьте в файл /etc/ntp.conf следующие строки (адреса вида rhel.pool.ntp.org указаны для примера):

```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```

Запустите NTP-сервер:

```
/etc/init.d/ntpd start
chkconfig ntpd on
```

1.3 Использование SSHv2

Для доступа к Service Console может применяться служба SSH. В таком случае требуется запретить использование небезопасных способов аутентификации, а также отключить некоторые другие опции из списка, приведенного ниже.

Настройка:

В файле /etc/ssh/sshd_config укажите следующие опции настройки:

```
Protocol 2
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
```

Для того чтобы изменения вступили в силу, требуется перезапуск SSHD:

```
/etc/init.d/sshd restart
```

1.4 Применение криптоалгоритма AES для SSH

Требуется применять криптоалгоритм AES для шифрования трафика SSH. Он более безопасен, чем использовавшийся ранее DES, и в отличие от Blowfish и других криптоалгоритмов (поддерживаемых библиотекой OpenSSL) поддерживается большим количеством клиентских устройств.

Настройка:

В конфигурационном файле /etc/ssh/sshd_config установите опцию Ciphers:

```
Ciphers aes256-cbc,aes128-cbc
```

Для того чтобы изменения вступили в силу, требуется перезапуск SSHD:

```
/etc/init.d/sshd restart
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1.5 Запрет входа пользователя root через SSH

В целях безопасности вход в систему по протоколу SSH с учетной записью суперпользователя root должен быть запрещен. Это позволит предотвратить атаки подбора пароля на данную учетную запись, а также упростит разбор внутренних инцидентов в случае, когда пароль к данной учетной записи известен более чем одному человеку.

Настройка:

В конфигурационном файле `/etc/ssh/sshd_config` установите опцию:

```
PermitRootLogin no
```

Для того чтобы изменения вступили в силу, требуется перезапуск SSHD:

```
/etc/init.d/sshd restart
```

1.6 Ограничение доступа к команде su

Команда su служит для запуска оболочки с правами указанного пользователя, чаще всего root. Следует предоставить доступ к данной команде только администраторам сервера Citrix XenServer, включив их в группу wheel и затем включив режим ограничения доступа, при котором выполнить команду su смогут только члены группы wheel.

Примечание. В зависимости от политики безопасности организации использование команды su может быть запрещено. В таком случае привилегированные операции необходимо выполнять при помощи sudo, и группа wheel должна быть пуста.

Настройка:

Для каждого пользователя (в данном примере это `admin`) выполните команду:

```
usermod -G wheel admin
```

Затем разрешите доступ к команде su только членам группы wheel. Для этого в файле `/etc/pam.d/su` должна присутствовать незакомментированная строка:

```
auth required pam_wheel.so use_uid
```

Если использование команды su запрещено, просмотрите файлы `/etc/passwd` (первичная группа) и `/etc/group` (вторичные группы) и убедитесь, что в группу wheel не входит ни один пользователь.

1.7 Запрет перехода в однопользовательский режим без пароля

Операционная система Citrix XenServer основана на RedHat Linux; соответственно, она также поддерживает однопользовательский режим, который можно активировать в настройках загрузчика. Если заданы настройки по умолчанию, то после загрузки данного режима пользователь получает консоль с правами root без пароля. Такой сценарий позволяет злоумышленнику, имеющему доступ к локальной консоли сервера Citrix XenServer, получить права root и выполнить на уязвимом сервере любые действия. Отсюда вытекает необходимость настроить ОС на запрос пароля пользователя root при переходе в однопользовательский режим.

Настройка:

В файле `/etc/inittab` отредактируйте имеющуюся строку, у которой во втором поле стоит символ “S”. Если такая строка отсутствует, добавьте в файл следующую запись:

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

```
~~:S:wait:/sbin/sulogin
```

1.8 Пароль загрузчика extlinux

Загрузчик операционной системы Citrix XenServer позволяет передать множество параметров загрузки ядру ОС при ее запуске, в том числе – команду перехода в однопользовательский режим. По умолчанию доступ к опциям загрузки ОС не защищен паролем, что позволяет злоумышленнику, имеющему физический доступ к локальной консоли управления Xen-сервером, передать загрузчику неавторизованные параметры запуска ОС. Чтобы избежать этого, требуется установить пароль для доступа к управлению загрузчиком. Файл конфигурации загрузчика сервисной консоли должен быть доступен только для операций чтения/записи и только суперпользователю системы root.

Настройка:

В Service Console от имени root выполните команды:

```
echo <пароль_загрузчика> | sha1sum
chown root:root /boot/extlinux.conf
chmod 600 /boot/extlinux.conf
```

После этого внесите полученные 40 символов хэша пароля в файл/boot/extlinux.conf (в глобальную секцию настроек загрузчика):

```
menu master passwd <password_sha1_hash>
```

1.9 Активация режима хранения паролей в файле /etc/shadow

В операционной системе Citrix XenServer по умолчанию в настройке модуля `pam_unix.so` отсутствует опция хранения хэшей паролей в отдельном файле (`/etc/shadow`). Таким образом, злоумышленник может получить доступ к хэшам паролей при наличии учетной записи в системе. Рекомендуется внести изменения в настройки системы для предотвращения подобного события.

Настройка:

Отредактируйте строку в файле /etc/pam.d/system-auth следующим образом:

```
password    sufficient    pam_unix.so try_first_pass use_authtok
nullok md5 shadow
```

Выполните команду:

```
pwconv
```

Перезагрузите операционную систему.

1.10 Проверка отсутствия пользователей с пустым паролем

Учетная запись пользователя с пустым паролем может быть использована злоумышленником для входа в систему. Все учетные записи в системе должны либо быть защищены паролем, либо заблокированы записью вида «!!». Пример записи в /etc/shadow:

```
vncterm_base:!!:15278:0:99999:7:::
```

Настройка:

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Установите пароли пользователям, если таковые отсутствуют. Для этого используйте команду passwd. Кроме того, заблокируйте неактивных пользователей, используя команду `usermod –L <username>`.

1.11 Проверка отсутствия символа «+» в файлах passwd, shadow и системных файлах групп

Символ «+» в системных файлах настроек учетных записей и паролей используется системой как маркер для вставки значения из NIS. Рекомендуется удалить подобные записи для обеспечения безопасности системы. Пример подобной записи из файла /etc/shadow:

```
username:+:15278:0:99999:7:::
```

Настройка:

Удалите символы «+» из служебных файлов.

1.12 Установка сертификатов сервера Citrix XenServer

Для предотвращения подмены сертификатов необходимо установить пользовательские сертификаты .pem SSL.

Настройка:

Для установки CA-сертификата выполните описанные ниже действия.

Подключите ключевой носитель к системе.

Выполните команду:

```
xe pool-certificate-install filename=</path/to/ca-cert.pem>
```

Здесь `</path/to/ca-cert.pem>` — путь к сертификату файла на внешнем носителе.

Для добавления сертификата сервера выполните описанные ниже действия.

Подключите ключевой носитель к системе.

Выполните следующие команды:

```
service xapi stop
pkill stunnel
cp /etc/xensource/xapi-ssl.pem /etc/xensource/orig-xapi-ssl.pem
cp /path/to/new/cert.pem /etc/xensource/xapi-ssl.pem
service xapi start
```

Для включения режима проверки SSL-сертификатов выполните команду:

```
touch /var/xapi/verify_certificates
```

1.13 Обновление пакетов, содержащих уязвимости

Как известно, операционная система Citrix XenServer базируется на дистрибутиве RedHat Linux 5-го поколения. Компания Citrix регулярно (раз в полгода) выпускает исправления безопасности (patch updates). При этом в дистрибутиве системы используются довольно старые версии пакетов. Несмотря на утверждения компании Citrix, что данные пакеты не имеют уязвимостей, рекомендуется проверять систему на наличие уязвимых пакетов самостоятельно, используя стороннее программное обеспечение.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Настройка:

Помните, что обновление уязвимых пакетов описанным методом пользователь выполняет на свой страх и риск. Работоспособность ОС после установки обновлений не гарантируется. Обязательно создайте резервную копию системы перед выполнением данных действий. Обновлять уязвимые пакеты должен специалист, способный самостоятельно решить возникшие проблемы в случае отказа **xapi** или других компонентов системы. Помните, что обновление не должно затрагивать группы пакетов, связанных с **udev**, **lvm2**, **xen** или ядром системы.

Выявите уязвимые пакеты в системе любым доступным вам способом.

Например, вы можете использовать сканер безопасности или проверить версии средствами плагина yum secure. Рассмотрим пример нахождения уязвимых пакетов и последующие действия оператора. Допустим, вы определили, что следующие пакеты содержат уязвимости:

```
<package_1>
<package_2>
<package_3>
```

Далее вам необходимо активировать репозиторий yum для установки обновления пакетов. Отредактируйте строки «enabled=» в файле /etc/yum.repos.d/CentOS-Base.repo:

```
[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$bas
earch&repo=os
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
exclude=kernel-xen*, *xen*
enabled=1

#released updates
[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$bas
earch&repo=updates
#baseurl=http://mirror.centos.org/centos/$releasever/updates/$basearch
/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
exclude=kernel-xen*, *xen*
enabled=1
```

При этом на время обновления необходимо отключить репозиторий Citrix в файле /etc/yum.repos.d/Citrix.repo:

```
enabled=0
```

Далее обновите уязвимые пакеты, используя инструмент yum:

```
yum update <package_1> <package_2> <package_3>
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1.14 Хранение истории паролей

Чтобы предотвратить повторное использование паролей в течение короткого периода времени, необходимо сохранять хэш-суммы нескольких предыдущих паролей. Рекомендуется хранить 10 последних паролей.

Примечание. В случае, когда пароль пользователя меняется администратором (root), его хэш не попадает в файл истории паролей.

Настройка:

Выполните следующие команды:

```
touch /etc/security/opasswd
chmod 600 /etc/security/opasswd
chown root:root /etc/security/opasswd
```

Затем в файле /etc/pam.d/system-auth добавьте строку:

```
password    required    pam_unix.so      remember=10
```

1.15 Настройка протоколирования неудачных попыток входа в систему и ограничение количества дополнительных попыток

Для ведения отчетов о попытках входа в систему рекомендуется включить дополнительное протоколирование ошибок входа в систему. Кроме того, необходимо блокировать пользователя на определенный период после ошибки аутентификации. Для этого следует соответствующим образом настроить модули аутентификации (PAM).

Настройка:
Отредактируйте файл /etc/pam.d/system-auth. Чтобы затруднить подбор паролей для доступа к системе, рекомендуется активировать модуль pam_tally. С указанными ниже настройками он будет блокировать пользователей на 300 секунд при троекратной ошибке пароля:

```
auth        required      pam_env.so
auth        required      pam_tally.so deny=3 unlock_time=300
even_deny_root_account
auth        sufficient    pam_unix.so try_first_pass nullok
auth        required      pam_deny.so

account     required      pam_unix.so
account     required      pam_tally.so
password    required      pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so try_first_pass use_authtok
nullok md5 shadow
password    required  pam_unix.so     remember=10
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session     required      pam_unix.so
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1.16 Установка срока действия паролей

Длина паролей пользователей для входа в систему должна составлять не менее 9 символов. Максимальный срок действия пароля необходимо ограничить 90 днями для уменьшения риска в случае компрометации. Оповещать пользователей рекомендуется за 14 дней до истечения срока действия пароля.

Настройка:
Для каждого существующего пользователя кроме администратора выполните команду:

```
chage -m 7 <имя_пользователя>
```

Для настройки парольной политики отредактируйте следующие строки в файле /etc/login.defs:

```
PASS_MAX_DAYS=90
PASS_MIN_DAYS=7
PASS_WARN_AGE=14
PASS_MIN_LEN=9
```

Убедитесь, что в файле `/etc/pam.d/system-auth` присутствует строка:

```
password required pam_cracklib.so try_first_pass retry=3
minlen=9,dcredit=-1,ucredit=-1,ocredit=-1 lcredit=-1
```

1.17 Настройка хранения системных журналов

По умолчанию операционная система XenServer хранит файлы системных журналов в корневом разделе системы. Данное решение является небезопасным, так как переполнение основного раздела вызывает сбой в работе системы. Для решения данного вопроса рекомендуется хранить файлы системного журнала в отдельном разделе.

Настройка:
Выполните следующую команду в консоли XenServer, чтобы получить UUID локальной группы томов:

```
xe sr-list name-label=Local\ storage params=uuid host=$HOSTNAME
```

Определите наличие свободного места в группе томов (замените UUID на полученный в предыдущей команде):

```
vgdisplay VG_XenStorage-<UUID> | grep Free
```

Если в группа томов имеется необходимое свободное пространство, выполните следующую команду для создания нового тома:

```
lvcreate VG_XenStorage-<UUID> -n LogLV -L 4G
```

Создайте файловую систему Ext3 на новом томе:

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

```
mkfs.ext3 /dev/VG_XenStorage-<UUID>/LogLV
```

Добавьте следующую запись в файл **/etc/fstab**:

```
/dev/VG_XenStorage-<UUID>/LogLV /var/log ext3 defaults 0 0
```

Создайте стартовый сценарий **/etc/rc3.d/S02loglv** со следующим содержанием:

```
#!/bin/bash
lvchange -a y VG_XenStorage-<UUID>/LogLV
```

Сценарий должен обладать правами на выполнение. Для этого выполните следующую команду:

```
chmod a+x /etc/rc3.d/S02loglv
```

Выполните приведенные ниже команды для подлючения файловой системы, перезапуска демона **syslog** и перемещения текущих файлов:

```
service syslog stop
mkdir /tmp_log
mv /var/log/* /tmp_log/
mount /dev/VG_XenStorage-<UUID>/LogLV /var/log
mv /tmp_log/* /var/log/
service syslog start
rm –rf /tmp_log/
```

Перезагрузите сервер. После перезагрузки выполните следующую команду, чтобы проверить, была ли новая файловая система подключена к **/var/log**:

```
mount | grep LogLV
```

1.18 Настройка каталога для хранения временных файлов

При базовой установке операционная система XenServer не выделяет отдельный раздел для каталога **/tmp**. Это является небезопасным, так как переполнение основного раздела вызывает сбой в работе системы. Кроме того, загрузчик **pygrub** использует **/tmp** в качестве временного хранилища для **kernel** и **initrd** при загрузке гостевых систем.

Настройка:
Выполните следующую команду в консоли XenServer, чтобы получить UUID локальной группы томов:

```
xe sr-list name-label=Local\ storage params=uuid host=$HOSTNAME
```

Определите наличие свободного места в группе томов (замените UUID на полученный в предыдущей команде):

```
vgdisplay VG_XenStorage-<UUID> | grep Free
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Если в группа томов имеется необходимое свободное пространство, выполните следующую команду для создания нового тома:

```
lvcreate VG_XenStorage-<UUID> -n TmpLV -L 4G
```

Создайте файловую систему Ext3 на новом томе:

```
mkfs.ext3 /dev/VG_XenStorage-<UUID>/TmpLV
```

Добавьте следующую запись в файл **/etc/fstab**:

```
/dev/VG_XenStorage-<UUID>/TmpLV /tmp ext3 defaults,nosuid,nodev,noexec
0 0
```

Создайте стартовый сценарий **/etc/rc3.d/S03tmplv** со следующим содержанием:

```
#!/bin/bash
lvchange -a y VG_XenStorage-<UUID>/TmpLV
```

Сценарий должен обладать правами на выполнение. Для этого выполните следующую команду:

```
chmod a+x /etc/rc3.d/S03tmplv
```

Перезагрузите сервер. После перезагрузки выполните следующую команду, чтобы проверить, была ли новая файловая система подключена к **/tmp**:

```
mount | grep TmpLV
```

2. НАСТРОЙКА СЕТЕВЫХ ПАРАМЕТРОВ СИСТЕМЫ

Предложенные ниже настройки являются абстрактным примером *для сферического гипервизора в вакууме* и могут меняться в зависимости от используемой сетевой архитектуры и специфики аппаратной части серверного оборудования.

2.1 Распределение сетевых интерфейсов по задачам

Для максимальной безопасности следует разделить сети для управления, передачи данных и основного назначения. Таким образом, можно избежать компрометации системы при попадании злоумышленника в одну из сетей. Идеология данного решения приведена на Рис.1.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

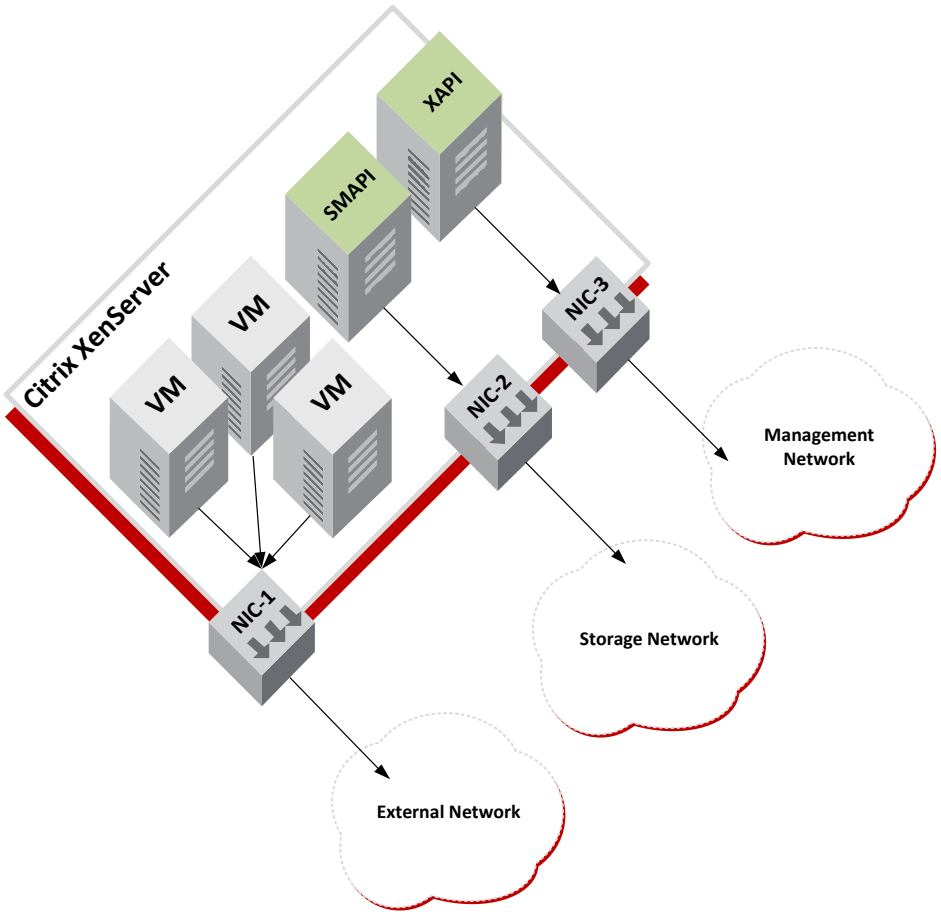

Рис. 1. Логическая схема разделения сетей гипервизора

Настройка:

При наличии нескольких сетевых интерфейсов разделите их физически и логически. Если такой возможности нет, то рекомендуется разделить их на уровне IP-адресации или другим способом.

Настройка интерфейса управления

Выведите список UUID PIF, относящихся к устройству eth0 (NIC0), и UUID его сети:

```
xe pif-list device=eth0 params=uuid,network-uuid
```

Измените название сети:

```
xe network-param-set uuid=<network uuid> name-label="Management NW"
```

Настройка интерфейса передачи данных

Выведите список UUID PIF, относящихся к устройству eth1 (NIC1), и UUID его сети:

```
xe pif-list device=eth1 params=uuid,network-uuid
```

Настройте IP-адрес сети:

```
# xe pif-reconfigure-ip uuid=<pif uuid>> mode=static IP=<ip> \
gateway=<gateway> netmask=<netmask> DNS=<DNS>
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Измените название сети:

```
xe network-param-set uuid=<network uuid> name-label="Storage NW"
```

Настройка интерфейса виртуальных машин
Выведите список UUID PIF, относящихся к устройству eth2 (NIC2), и UUID его сети:

```
xe pif-list device=eth2 params=uuid,network-uuid
```

Настройте режим отсутствия IP-адреса для гостевой сети:

```
xe pif-reconfigure-ip uuid=<uuid> mode=none
```

Измените название сети:

```
xe network-param-set uuid=<network uuid> name-label= "Guest NW 0"
```

Выполните аналогичные операции для eth3, eth4 и так далее.

2.2 Запрет использования нешифрованных подключений к XAPI

Стек XAPI по умолчанию ожидает подключения к порту 80 (по незашифрованному каналу) и порту 443 (по SSL-тоннелю). Если данные при установлении такого соединения не шифруются, то действия администратора системы могут быть скомпрометированы. Рекомендуется отключить доступ к порту 80 для всех клиентов за исключением рабочей станции, на которой установлен XenCenter.

Настройка:
Выполните команду:
`/etc/init.d/iptables save`
Отредактируйте следующую строку в файле /etc/sysconfig/iptables:

```
-A RH-Firewall-1-INPUT –s <xen_center_ip> -p tcp -m state --state NEW -
m tcp --dport 80 -j ACCEPT
```

Выполните команду:
`/etc/init.d/iptables restart`

2.3 Использование зашифрованных соединений в сети передачи данных

В операционной системе Citrix XenServer при переносе виртуальных машин с одного сервера на другой (например, в режиме XenMotion) данные передаются в незашифрованном виде. Даже в случае разделения сетей необходимо обеспечить защиту данного трафика. Для этого рекомендуется применить средства шифрования на IP-уровне, такие как VPN. Пример конкретной настройки здесь приведен не будет из-за многообразия возможных решений.

В случае с iSCSI-трафиком используется программное обеспечение OpenISCSI для подключения к удаленным iSCSI-хранилищам. Данное ПО поддерживает протокол CHAP для передачи пароля. Рекомендуется, чтобы подключение OpenISCSI использовало CHAP для аутентификации.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Настройка:
Для настройки CHAP-аутентификации для iSCSI-хранилища рекомендуется обратиться к соответствующей документации, поставляемой с конкретным программно-аппаратным решением. При настройке SR на клиентском узле необходимо в явном виде указать данные CHAP:

```
xe sr-create host-uuid=<valid_uuid> content-type=user \
name-label=<"Example shared LVM over iSCSI SR"> shared=true \
device-config:target=<target_ip=> device-
config:targetIQN=<target_iqn=> \
device-config:SCSIid=<scsci_id> \
device-config:chapuser=<chap_user> \
device-config:chappassword=<chap_password> \
type=lvmoiscsi
```

2.4 Настройка umask при создании файлов виртуальных машин в системе

По умолчанию ОС Citrix XenServer создает файлы виртуальных машин с правом чтения для категории пользователей “other”. Таким образом, любой пользователь системы имеет возможность получить доступ к данным виртуальных машин.
Следует ограничить права доступа к файлам данного типа.

Настройка:
Чтобы изменить umask, внесите изменения в сценарии сервера.
Отредактируйте строчки в файле /opt/xensource/sm/FileSR.py:

```
def create(self, sr_uuid, vdi_uuid, size):
os.umask(077)
if util.ioretry(lambda: util.pathexists(self.path)):
```

Далее необходимо произвести компиляцию файлов pyc и pyo. Для этого создайте файл /opt/xensource/sm/compile.py следующего содержания:

```
#!/usr/bin/python
import py_compile
py_compile.compile('/opt/xensource/sm/FileSR.py')
```

Далее выполните команды:

```
python /opt/xensource/sm/compile.py
python -O /opt/xensource/sm/compile.py
```

В качестве завершающего шага перезагрузите гипервизор, используя следующую команду:

```
shutdown -r now
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

2.5 Настройка удаленного NFS-хранилища

Каждое удаленное хранилище NFS-типа представляет собой каталог, содержащий файл формата VHD. Формат VHD не подразумевает шифрование данных, поэтому рекомендуется строго ограничить список клиентов, которым разрешено подключать данный каталог.

Настройка:
Для работы с удаленным NFS-хранилищем рекомендуется внести изменения в настройки сервера. В данном руководстве мы рассмотрим настройку NFS-хранилища на удаленном сервере Linux. Просмотрите файл /etc/exports и убедитесь в том, что подключение к серверу возможно только с определенного узла:

```
/<vm_share_dir>
<xenserver_ip>(rw,root_squash,anonuid=<xen_user_UID>,anongid=<xen_user
_GID>,sync)
```

Установите принадлежность каталога:

```
chown <xen_user>:<xen_user_group> <vm_share_dir>
```

Настройте демонов mountd, statd, lockd и rquotad для работы на статических портах (порты 4002-4006 указаны для примера) в файле /etc/sysconfig/nfs:

```
MOUNTD_PORT=”4002”
STATD_PORT=”4003”
LOCKD_TCPPORT=”4004”
LOCKD_UDPPORT=”4004”
RQUOTAD_PORT=”4005”
STATD_OUTGOING_PORT=”4006”
```

Добавьте следующие записи в таблицу INPUT сетевого фильтра /etc/sysconfig/iptables:

```
Iptables –A INPUT –s  <xenserver-ip> -p tcp –dport 111 –j ACCEPT
Iptables –A INPUT –s  <xenserver-ip> -p udp –dport 111 –j ACCEPT
Iptables –A INPUT –s  <xenserver-ip> -p tcp –dport 4002:4006 –j ACCEPT
Iptables –A INPUT –s  <xenserver-ip> -p udp –dport 4002:4006 –j ACCEPT
Iptables –A INPUT –s  <xenserver-ip> -p tcp –dport 2049 –j ACCEPT
Iptables –A INPUT –s  <xenserver-ip> -p udp –dport 2049 –j ACCEPT
```

2.6 Отключение возможности использования смешанного режима сетевых карт виртуальных машин

При включенном смешанном режиме (promiscuous mode) симулируемого сетевого интерфейса виртуальная машина имеет возможность перехватывать трафик других гостевых систем, а также использовать другие специфичные для данного режима функции, в том числе возможности по отсылке некорректных или вредоносных запросов (случайно или преднамеренно). Рекомендуется не включать данный режим, если это не требуется.

Настройка:
Для отключения смешанного режима VIF выполните следующие команды в Service Console:

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

```
xe pif-param-set uuid=<PIF UUID> other-config:promiscuous="off"
```
или:
```
xe pif-param-set uuid=<PIF UUID> other-config:promiscuous="false"
```

2.7 Настройка сетевых параметров ядра ОС

Для повышения устойчивости Citrix XenServer к сетевым атакам требуется настроить следующие параметры ядра ОС:

```
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Настройка:
Для применения данных настроек внесите их в файл /etc/sysctl.conf. После этого перезагрузите систему или выполните команду:
```
sysctl -p
```

2.8 Настройка межсетевого экрана

В стандартный комплект поставки Citrix XenServer входит межсетевой экран Netfilter и утилита командной строки iptables для управления его работой. Чтобы обеспечить безопасность сетевого взаимодействия, необходимо настроить данное программное обеспечение.

Настройка:
Используйте следующие настройки для сети управления:

```
service iptables start
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
iptables -A INPUT -i xenbr0 -p tcp --dport 443 -m state --state NEW -j
ACCEPT
iptables -A INPUT -i xenbr0 -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A INPUT -i xenbr0 -j DROP
iptables -A OUTPUT -o xenbr0 -p tcp --dport 443 -m state --state NEW -
j ACCEPT
iptables -A OUTPUT -o xenbr0 -p tcp --dport 7279 -m state --state NEW
-j ACCEPT
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

```
iptables -A OUTPUT -o xenbr0 -p tcp --dport 27000 -m state --state NEW
-j ACCEPT
iptables -A OUTPUT -o xenbr0 -p udp --dport 123 -m state --state NEW -
j ACCEPT
iptables -A OUTPUT -o xenbr0 -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o xenbr0 -j DROP
```

Входящая цепочка для сети передачи данных:

```
iptables -A INPUT -i xenbr1 -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A INPUT -i xenbr1 -j DROP
```

Для настройки удаленного подключения к серверу NFS (в качестве примера рассмотрен конкретный сервер) добавьте следующие разрешения:

```
iptables -A OUTPUT -o xenbr1 -p udp --dport 111 -m state --state NEW -
j ACCEPT
iptables -A OUTPUT -o xenbr1 -p tcp --dport 111 -m state --state NEW -
j ACCEPT
iptables -A OUTPUT -o xenbr1 -p udp --dport 2049 -m state --state NEW
-j ACCEPT
iptables -A OUTPUT -o xenbr1 -p tcp --dport 2049 -m state --state NEW
-j ACCEP
iptables -A OUTPUT -o xenbr1 -p udp --dport 4002:4006 -m state --state
NEW -j ACCEPT
iptables -A OUTPUT -o xenbr1 -p tcp --dport 4002:4006 -m state --state
NEW -j ACCEPT
iptables -A OUTPUT -o xenbr1 -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o xenbr1 -j DROP
```

Для подключения к альтернативным удаленным хранилищам добавьте собственные правила. Завершите настройку:

```
service iptables save
chkconfig iptables on
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

3. НАСТРОЙКИ ГИПЕРВИЗОРА XENSERVER

Данный раздел содержит информацию о специфичной настройке, корректировке существующих параметров и изменении критических файлов внутреннего демона XAPI и его окружения. Предложенные модификации могут повлиять на работоспособность виртуальной инфраструктуры и не рекомендуются к исполнению на серверах, находящихся в промышленной эксплуатации.

3.1 Отключение режима debug для xenstored

Данное ограничение необходимо ввести, чтобы запретить использование гостевыми системами режима debug.

Настройка:
Удалите запись вида allow-debug=true из файла /etc/xensource/xenstored.conf.

3.2 Настройка распределенного секрета для режима pool

Выполняется на системе, являющейся pool-master. Данная настройка применяется для того, чтобы затруднить подмену сертификата, использующегося для внутрисистемного обмена информацией. Для этого необходимо создать новый сертификат, используя генератор случайных чисел, который обеспечивает достаточный уровень энтропии.

Настройка:
Для создания токена выполните следующие команды:

```
service xapi stop
rm /etc/xensource/ptoken

(ent=$(cat /proc/sys/kernel/random/entropy_avail); while [[ $ent -lt
2000 ]]; do \
sleep 15; ent=$(cat /proc/sys/kernel/random/entropy_avail); done) && \
service xapi start
```

3.3 Отключение режима debug для демона xapi

В системе по умолчанию включен режим Global Catalog Debug. Так как данная функция является избыточной, рекомендуется превентивно отключить ее, чтобы избежать компрометации данных системы.

Настройка:
В файле /etc/xensource/xapi.conf измените значение следующего параметр на `false`:

```
gc-debug = true
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

3.4 Настройка протоколирования демона xenstored

Рекомендуется настроить протоколирование действий демона xenstored, чтобы обеспечить возможность анализа в случае компрометации системы. Обращаем Ваше внимание на то, что необходимо настроить ротацию данного системного журнала.

Настройка:
Отредактируйте следующие строки в файле /etc/xensource/xenstored.conf:

```
# Logs
#log = error;general;file:/var/log/xenstored.log
log = warn;general;file:/var/log/xenstored.log
#log = info;general;file:/var/log/xenstored.log
#log = debug;io;file:/var/log/xenstored-io.log
```

3.5 Запрет автоматического входа vncterm в dom0 с правами суперпользователя

Если используется локальная авторизация без подсистемы RBAC с привязкой средствами Active Directory (в версиях Free, Advanced), то при создании запроса в XAPI на подключение к текстовой консоли гипервизора происходит автоматический вход в систему с правами суперпользователя root независимо от того, какой пользователь XAPI запросил выполнение данной операции. Чтобы обеспечить безопасность системы, необходимо запретить возможность подобного входа в систему, изменив опцию автоматического входа на стандартный login prompt, переадресовав вызов службе SSH.

Настройка:
Отредактируйте следующие строки в файле /usr/lib/xen/bin/dom0term.sh (здесь <admin_user> — ваша административная учетная запись, а не root):

```
#! /bin/bash

read -s -p "Press <Enter> to login
" ignore
clear
exec ssh <admin_user>@localhost
```

3.6 Отключение автозагрузки xsconsole под учетной записью root на tty1

При загрузке системы на физическую консоль по умолчанию выводится консоль Xsconsole, запущенная с привилегиями root. Для предотвращения инъекции sh-кода и\или перехвата сессии через тестовый режим необходимо изменить сценарий автоматической загрузки.

Настройка:
Откройте файл /opt/xensource/libexec/run-boot-xsconsole для редакции и измените строку вызова терминала, как описано ниже.

Исходная строка:

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

```
exec /sbin/mingetty --noissue --autologin root --
loginprog=/usr/bin/xsconsole $TTY

Измененная строка:

exec /sbin/mingetty --noissue --autologin nobody --
loginprog=/usr/bin/xsconsole $TTY
```

3.7 Настройка PAM-модуля для XAPI

По умолчанию любой пользователь ОС Citrix XenServer (в версиях Free, Advanced) имеет право подключиться к XAPI с полномочиями pool-admin. Это обусловлено спецификой продукта. Так как это позволяет, по сути, любому пользователю совершать любые операции с системой, используя Xen API, то необходимо ограничить список пользователей, допущенных к XAPI, средствами модуля PAM.

Настройка:
Войдите в систему как суперпользователь root и создайте файл /etc/xapi_allow с записью «root» в первой строке. Используя перенос строки в качестве разделителя, перечислите всех допущенных к XAPI пользователей.
Отредактируйте файл /etc/pam.d/xapi таким образом, что бы он имел следующий вид:

```
#%PAM-1.0
auth        required      pam_env.so
auth        required      pam_listfile.so item=user sense=allow
file=/etc/xapi_allow
auth        sufficient    pam_unix.so try_first_pass nullok
auth        required      pam_deny.so

account     required      pam_unix.so

password    required      pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so try_first_pass use_authtok
nullok md5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session     required      pam_unix.so
```

После внесения данных изменений доступ к XAPI смогут получить только пользователи из списка xapi_allow:

```
root
admin
user
```

Кроме того, необходимо ограничить доступ к следующему файлу:

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

```
chmod 600 /etc/xapi_allow
```

3.8 Проверка testing-режима xsconcole

При добавлении в каталог /usr/lib/xsconsole/ файла с названием testing.txt программа Xsconsole запустится в тестовом режиме. Если в файле testing.txt буду обнаружены переменные «host=» и «password=», то программа xsconsole будет пытаться выполнить аутентификацию на удаленном сервере. При этом в случае использования программы xsconsole на локальной консоли tty1 возможно получение доступа к локальной консоли с правами суперпользователя root.

Настройка:
Проверьте, что файл /usr/lib/xsconsole/testing.txt отсутствует.
Если он существует — удалите его.

3.9 Запрет стандартной страницы веб-сервера

По умолчанию в системе работает веб-сервер, позволяющий загружать файлы программы XenCenter и указывающий текущую версию системы. Чтобы избежать разглашения версии системы, рекомендуется удалить данную страницу полностью или изменить содержащуюся в ней информацию.

Настройка:
Скорректируйте индексный файл веб-сервера Citrix-index.html в каталоге /opt/xensource/www:

```
<html>
  <title>XenServer 5.6.0</title>
<head>
</head>
<body>
  <p/>Citrix Systems, Inc. XenServer 5.6.0
  <p/><a href="XenCenter.iso">XenCenter CD image</a>
  <p/><a href="XenCenter.msi">XenCenter installer</a>
</body>
</html>
```

Замените приведенные выше строки на:

```
<html>
</html>
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.