ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по безопасной настройке виртуальной инфраструктуры, построенной на базе программного обеспечения VMware

2026

1. Обеспечить сбор, запись и хранение журналов событий всех компонентов виртуальной инфраструктуры (VMware ESXi, vCenter) путем настройки ведения журналов событий.

На хостах VMware ESXi функционирует служба Syslog (vmsyslogd), которая обеспечивает стандартный механизм регистрации сообщений от ядра виртуальной машины и других компонентов системы. По умолчанию в ESXi эти журналы хранятся на локальном временном томе или в оперативной памяти. Для дальнейшего хранения журналов ESXi возможно настроить размещение этих журналов в альтернативном месте на диске и отправку журналов по сети на сервер Syslog.

Настройка может быть осуществлена с использованием консоли «ESXi Shell», профилей хоста и веб-клиента vSphere.

Существует пять настраиваемых параметров журналов событий ESXi:

Syslog.global.logDir - расположение в локальном или удалённом хранилище данных (VMFS, NFS, FAT) и путь, по которому должны сохраняться журналы. Для версий ESXi 6.7 и выше каталог журналов должен быть создан до настройки глобального параметра каталога журналов.

Syslog.global.logHost — список удалённых серверов, разделённых запятыми, на которые отправляются логи по протоколу syslog. Если поле logHost не заполнено, логи не пересылаются.

Syslog.global.logDirUnique - логический параметр, который определяет, создается ли каталог для конкретного хоста в настроенном logDir. Имя каталога - это имя хоста хоста ESXi. По умолчанию используется значение «false».

Syslog.global.defaultRotate — максимальное количество файлов журнала, которые можно хранить локально на хосте ESXi в настроенном каталоге logDir. По умолчанию 8.

Syslog.global.defaultSize — максимальный размер в килобайтах каждого локального файла журнала перед его ротацией. По умолчанию - 1024 Кб.

1.1 Для настройки локального и удаленного ведения журнала событий с помощью команды «*esxcli*» необходимо выполнить следующие действия:

открыть консоль «ESXi Shell», в которой доступна команда «*esxcli*», например, в vCLI или непосредственно на хосте ESXi;

выполнить команду:

esxcli system syslog config get;

задать новую конфигурацию хоста, указав новые параметры для изменения, например:

esxcli system syslog config set --logdir=/path/to/vmfs/directory/ --loghost=RemoteHostname --logdir-unique=true|false --default-rotate=NNN --default-size=NNN

Пример: для настройки удалённого системного журнала событий с использованием TCP на порту 514 необходимо выполнить команду:

esxcli system syslog config set –loghost='tcp://10.11.12.13:514';

после внесения изменений в конфигурацию, необходимо выполнить перезагрузку службы командой:

esxcli system syslog reload;

для проверки доступности порта с хоста ESXi необходимо выполнить команду:

nc -z RemoteHostname 514

Пример: *nc -z 10.11.12.13 514.*

1.2 Для настройки локального и удаленного ведения журнала событий с использованием профилей хоста необходимо выполнить следующие действия:

подключиться к серверу vCenter с помощью клиента vSphere;

выбрать раздел «Home»;

далее в разделе «Management» выбрать «Host Profiles»;

создать новый профиль или отредактировать существующий профиль;

в окне «Edit Profile» задать один или несколько из пяти параметров конфигурации;

сохранить профиль и назначить его хостам.

Справочно: если настройка журнала событий с помощью esxcli или расширенных параметров конфигурации уже была произведена и указанный

профиль использовался в качестве эталонного, то 5 параметров конфигурации уже должны отображаются в разделе «Advanced Configuration options»;

если журнал событий не был настроен ранее, необходимо нажать правой кнопкой мыши на раздел «Advanced Configuration options» и добавить профиль для каждого из пяти параметров конфигурации.

1.3 Для настройки локального и удаленного ведения журнала событий с использованием профилей хоста с помощью веб-клиента vSphere необходимо выполнить следующие действия:

подключиться к серверу vCenter с помощью веб-клиента vSphere;

выбрать раздел «Home»;

в разделе «Operations and Policies» выбрать «Host Profiles»;

создать новый профиль или отредактировать существующий профиль;

в окне «Edit Profile» задать один или несколько из пяти параметров конфигурации;

сохранить профиль и назначить его хостам.

2. Обеспечить переадресацию журналов событий всех компонентов виртуальной инфраструктуры (VMware ESXi, vCenter) на удаленный сервер, чтобы исключить возможность их изменения или уничтожения злоумышленниками.

Для настройки переадресации журналов событий на удаленный сервер необходимо выполнить следующие действия:

в консоли хоста ESXi выполнить следующие команды:

Esxcli system syslog config set –loghost=’<remote_host>’;

после внесения изменений в конфигурацию, необходимо выполнить перезагрузку службы командой:

Esxcli system syslog reload;

предоставить доступ к трафику журнала событий через встроенный межсетевой экран командой:

Esxcli network firewall ruleset set –ruleset-id=syslog –enabled=true.

3. Обеспечить передачу в SIEM-ситсему журналов событий всех компонентов виртуальной инфраструктуры (VMware ESXi, vCenter) и организовать их мониторинг.

Необходимо осуществлять мониторинг журналов событий, представленных в таблице 1, где:

Наименование директории — это путь к файлу, в котором хранятся записи событий;

Назначение — это описание событий, записываемых в указанный файл;

Сообщение — это записи в файлах, описывающие регистрируемое событие;

Описание — это описание регистрируемых событий.

Таблица 1 — Перечень журналов событий.

Наименование директории	**Назначение**	**Сообщение**	**Описание**
Использование службы SSH для ESXi			
var/log/shell.log	Журналы использования оболочки ESXi, Shell включая включение/ отключение и каждую введенную команду	Accepted password for user <username> from <source IP> [Auth]: User <username> User <username>@<source IP> logged in as <User Agent>	Аутентификация в веб-консоли ESXi
/var/log/vobd.log	События в ядре VM	SSH access has been enabled	Включение SSH-доступа для ESXi на веб-консоли
/var/log/hostd-probe.log	Проверка работоспособности службы управления хостом	eventTypeId = “esx.audit.ssh.enabled” SSH access has been enabled SSH for the host localhost.localdomain has been enabled	Включение SSH-доступа для ESXi на веб-консоли

Наименование директории	**Назначение**	**Сообщение**	**Описание**
/var/log/auth.log	Успешная и неудачная аутентификация в ESXi Shell.	SSH login enabled	Включение SSH-доступа для ESXi на веб-консоли
Изменение правил встроенного межсетевого экрана ESXi			
/var/log/vobd.log	События в ядре VM	Firewall configuration has changed. Operation ‘disable’ for rule set snmp succeeded	Отключение правил межсетевого экрана через веб-консоль или через оболочку
/var/log/hostd-probe.log	Проверка работоспособности службы управления хостом	Task Created : haTask-ha-host-vim.host.FirewallSystem.disableRuleset- Firewall configuration has changed. Operation ‘disable’ for rule set succeeded Task Completed : haTask-ha-host-vim.host.FirewallSystem.disableRuleset-Status success	Отключение правил межсетевого экрана через веб-консоль
var/log/shell.log	Журналы использования оболочки ESXi, Shell включая включение/ отключение и каждую введенную команду	esxcli network firewall ruleset set –ruleset-id=<ruleset> –enabled=False	Отключение правил межсетевого экрана через ssh-оболочку
SSH-вход в ESXi			
/var/log/hostd-probe.log	Проверка работоспособности службы управления хостом	SSH session was opened for <username>@<source IP>	Аутентификация по SSH в ESXi
var/log/shell.log	Журналы использования оболочки ESXi, Shell	Interactive shell session started	Аутентификация по SSH в ESXi

Наименование директории	Назначение	Сообщение	Описание
	включая включение/ отключение и каждую введенную команду		
/var/log/auth.log	Успешная и неудачная аутентификация в ESXi Shell.	FIPS mode initialized Connection from <source IP> port <source port> Accepted keyboard-interactive/pam for root from <source IP> port <source port> ssh2 session opened for user <username> by (uid=0)	Аутентификация по SSH в ESXi
/var/log/vobd.log	События в ядре VM	SSH session was opened for '<username>@<source IP>'	Аутентификация по SSH в ESXi
Переадресация портов SSH			
var/log/shell.log	Журналы использования оболочки ESXi, Shell включая включение/ отключение и каждую введенную команду	ssh -fN -R 127.0.0.1:48000 support@192.168.134.130	Командная строка для переадресации портов SSH
Доступ к директории /vmfs/ и томам			
var/log/shell.log	Журналы использования оболочки ESXi, Shell включая включение/ отключение и каждую введенную команду	ls /vmfs/volumes cd datastore1/	Обход файловой системы ESXi
Добавление нового пользователя и назначение ролей пользователям			
/var/log/hostd-probe.log	Проверка работоспособности службы управления хостом	Task Created: haTash-ha-folder-root-vim.host.LocalAccountManager.create User-<numerical ID>	Создание пользователя через веб-консоль

Наименование директории	Назначение	Сообщение	Описание
		User lookup failed for ‘<new username>’ Account <username> was created on host <ESXi hostname> Task Completed: haTash-ha-folder-root-vim.host.LocalAccountManager.create User-<numerical ID> Status success	
/var/log/hostd-probe.log	Проверка работоспособности службы управления хостом	Task Created : haTash–vim.AuthorizationManager.setEntity Permissions-<numerical ID> Task Completed : haTash–vim.AuthorizationManager.setEntity Permissions-<numerical ID> Status success Permission created for <new username> on <username>, role is <assigned role>, propagation is Enabled	Назначение разрешений пользователям через веб-консоль

4. Организовать оповещение администраторов безопасности органа (организации) посредством SIEM-системы о наступлении следующих событий:

отключение виртуальных машин;

выполнение команд *./encryptor*, *sudo ./encryptor, *encryptor/vmfs/volumes*;

попытки входа с удаленных, заблокированных учетных записей пользователей;

создание новых учетных записей;

изменение административных привилегий Active Directory (идентификаторы событий 4728, 4732, 4756);

установка неизвестных программных пакетов (Vmware Installation Bundles);

изменение конфигурации хостов ESXi;

изменения пароля учетной записи root;

добавление хостов ESXi в Active Directory.

5. Осуществлять резервное копирование виртуальной инфраструктуры (VMware ESXi, vCenter), руководствуясь следующими принципами:

создавать и хранить не менее трех резервных копий информации – одну основную и две резервные;

использовать для хранения резервных копий не менее двух разных типов носителей информации (например, внешние жесткие диски и систему хранения данных);

хранить одну из резервных копий в отдельном (обособленном) от иных резервных копий месте;

хранить резервные копии в изолированном от сети «Интернет» сегменте информационной системы.

6. Организовать доступ пользователей, в том числе с административными правами, к виртуальной инфраструктуре ESXi с применением многофакторной аутентификации.

7. Исключить доступ к виртуальной инфраструктуре органа (организации) привилегированных пользователей по протоколу удаленного доступа SSH, в том числе под учетной записью root.

Для ограничения доступа по протоколу SSH необходимо выполнить следующие действия:

открыть консоль «ESXi Shell», в которой доступна команда «esxcli», например, в vCLI или непосредственно на хосте ESXi;

выполнить команды:

esxcli system ssh set --enabled=false

esxcli system shell set --enabled=false.

8. В случае невозможности исключения доступа к виртуальной инфраструктуре органа (организации) привилегированных пользователей по протоколу удаленного доступа SSH, организовать аутентификацию пользователей по SSH-ключам, а также настроить ограничение времени такого доступа.

Настройка ограничения времени доступа по протоколу удаленного доступа

SSH может быть осуществлена с использованием пользовательского интерфейса консоли «Direct Console User Interface (DCUI)» и веб-клиента vSphere.

8.1 Для настройки ограничения времени доступа SSH с использованием пользовательского интерфейса консоли «DCUI» необходимо выполнить следующие действия:

открыть пользовательский интерфейс «DCUI»;

выбрать Customize System/View Logs путем нажатия клавиши «F2»;

выбрать раздел «Troubleshooting Options» путем нажатия клавиши «Enter»;

выбрать раздел «Modify ESXi Shell and SSH timeout» путем нажатия клавиши «Enter»;

установить необходимое значение ограничения времени доступа в минутах.

Справочно: для осуществления указанной настройки необходимо предварительно отключить ESXi Shell и SSH-службы.

8.2 Для настройки ограничения времени доступа SSH с использованием веб-клиента vSphere необходимо выполнить следующие действия:

подключиться к веб-клиенту vSphere;

выбрать необходимый узел;

в разделе «Configuration» выбрать «Advanced Settings»;

установить параметру «UserVars.ESXiShellTimeOut» необходимое значение ограничения времени доступа в минутах;

установить параметру «UserVars.ESXiShellInteractiveTimeOut» необходимое значение ограничения времени доступа в минутах.

Кроме того, необходимо настроить ограничения времени доступа к пользовательскому интерфейсу консоли «DCUI», выполнив следующие действия:

подключиться к веб-клиенту vSphere;

выбрать необходимый узел;

перейти в разделы «Configure/Manage» - «Settings» - «System» - «Advanced System Settings»;

установить параметру «UserVars.DCUITimeOut» необходимое значение ограничения времени доступа в минутах.

9. Ограничить использование службы VMware Network API, выполнив следующие действия:

подключиться к веб-клиенту vSphere;

выбрать необходимый узел;

перейти в разделы «Configuretion» - «Advanced Settings» - «Net»;

если на выбранном узле не используются сетевые устройства безопасности, работающие на базе DVFilter, то установить параметру Net.DVFilterBindIpAddress пустое значение;

если на выбранном узле используются сетевые устройства безопасности, работающие на базе DVFilter, то установить параметру Net.DVFilterBindIpAddress соответствующий IP-адрес сетевого устройства.

Справочно: указанную настройку необходимо осуществить для каждого узла ESXi.

10. Заблокировать возможность установки программных пакетов (Vmware Installation Bundles) на хосты ESXi с помощью настройки строгой проверки подписи.

Для настройки строгой проверки подписи программных пакетов (Vmware Installation Bundles) необходимо выполнить следующие действия:

открыть консоль «ESXi Shell», в которой доступна команда «esxcli», например, в vCLI или непосредственно на хосте ESXi;

выполнить команду *esxcli software acceptance set — level=VMwareCertified.*

Кроме того, необходимо осуществлять проверку целостности программных пакетов (Vmware Installation Bundles) с использованием контрольных сумм.

11. Ограничить (по возможности) использование в виртуальной инфраструктуре служб HTTPS (порт 443), клиента vSphere для консоли (порт 902 TCP/UDP) и vMotion (TCP 8000).

12. Осуществлять регулярные обновления программного обеспечения VMware в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России

30 июня 2025 г. (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty).

13. Осуществлять работы в виртуальной инфраструктуре под учетными записями, имеющими минимально необходимые привилегии.

14. Обеспечить регулярную смену паролей привилегированных пользователей виртуальной инфраструктуры.

15. Осуществить настройку безопасной загрузки и принудительного использования безопасного режима в ESXi.

Для настройки безопасной загрузки и принудительного использования безопасного режима ESXi необходимо выполнить следующие действия:

открыть консоль ESXi Shell, в которой доступна команда «esxcli», например, в vCLI или непосредственно на хосте ESXi;

выполнить следующую команду *esxcli system settings encryption get*;

ответ, который должен быть отображен:

Mode: TPM

Require Executables Only From Installed VIBs: false

Require Secure Boot: true;

если в графе *«Require Secure Boot» стоит значение true* – настройка произведена;

если в графе *«Require Secure Boot» стоит значение false* – настройка не произведена;

если в графе *«Require Secure Boot» стоит значение none – необходимо* выполнить команду *esxcli system settings encryption set –mode=TPM.*

Для включения безопасной загрузки необходимо выполнить следующие команды:

отключить хост ESXi;

ввести команду *esxcli system settings encryption set –require-secure-boot=T;*

перезапустить хост ESXi;

проверить изменения командой *esxcli system settings encryption get* и убедиться, что в графе *«Require Secure Boot»* установлено *true;*

если в графе *«Require Executables Only From Installed VIBs»* - стоит значение *true* – настройка произведена;

если в графе *«Require Executables Only From Installed VIBs»* - стоит значение *false* – настройка не произведена.

Для включения принудительного использования безопасного режима необходимо выполнить следующие команды:

отключить хост ESXi;

выполнить команду *esxcli system settings kernel set -s execInstalledOnly -v TRUE;*

перезапустить хост ESXi;

выполнить команду *esxcli system settings encryption set –require-exec-installed-only=T;*

проверить изменения командой *esxcli system settings encryption get* и убедиться, что в графе *«Require Executables Only From Installed VIBs»* установлено *true.*

16. Активировать флаг «execInstalledOnly» на всех хостах ESXi в виртуальной среде для блокировки запуска любого неподписанного кода на хосте ESXi.

17. Обеспечить корректную настройку политик безопасности Portgroup для каждой группы портов на виртуальном коммутаторе с использованием vSphere Web Client путем выполнения следующих действий:

перейти в разделы «Configure/Manage» - «Settings» - «Policies»;

выбрать «Edit» и в разделе «Security» установить для политик «Forged transmits», «MAC Address Changes», «Promiscuous Mode» значение «Reject».

18. Выделить наиболее критичные компоненты виртуальной инфраструктуры в отдельный сегмент от других ресурсов и серверов органа (организации) с использованием межсетевого экрана.

19. Организовать на уровне сетевых средств защиты доступ к хостам ESXi, используя схему доступа по «черным» или «белым» спискам.