

Руководство по безопасной конфигурации

24 октября 2019 г.

vRealize Automation 7.5



vmware®

Актуальная техническая документация доступна на веб-сайте VMware:

<https://docs.vmware.com/ru/>

Все замечания по данной документации можно отправлять по адресу:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Россия
Россия, 125284, г. Москва
ул. Беговая, д.3, стр.1
Бизнес-центр "NORDSTAR TOWER" 30й этаж
Телефон: +7 495 212 29 00
www.vmware.com/ru

© 2015–2019 гг. VMware, Inc. Все права защищены. [Информация об авторских правах и товарных знаках.](#)

Содержание

1	Безопасная конфигурация	5
2	Обзор базового плана безопасности vRealize Automation	6
3	Проверка целостности установочного носителя	8
4	Усиление защиты инфраструктуры программного обеспечения системы VMware	9
	Усиление защиты среды VMware vSphere®	9
	Усиление защиты узла инфраструктуры как услуги	10
	Усиление защиты Microsoft SQL Server	10
	Усиление защиты Microsoft .NET	10
	Усиление защиты Microsoft Internet Information Services (IIS)	11
5	Проверка установленного программного обеспечения	12
6	Инструкции и исправления для системы безопасности VMware	13
7	Безопасная конфигурация	14
	Обеспечение безопасности устройства vRealize Automation	14
	Изменение пароля пользователя root	14
	Проверка сложности и хэша пароля пользователя Root	15
	Проверка журнала паролей пользователей root	15
	Управление сроком действия пароля	16
	Управление учетными записями SSH и администратора	17
	Изменение пользователей в интерфейсе управления виртуального устройства	21
	Настройка проверки подлинности загрузчика	22
	Настройка NTP	22
	Настройка TLS для передачи данных устройства vRealize Automation	23
	Проверка безопасности неактивных данных	31
	Настройка ресурсов приложения vRealize Automation	32
	Настройка конфигурации прокси-сервера консоли	35
	Настройка заголовков ответов сервера	37
	Настройка времени ожидания сеанса Устройство vRealize Automation	38
	Управление вспомогательным программным обеспечением	39
	Защита компонента инфраструктуры как услуги	43
	Настройка протокола NTP	43
	Настройка TLS для передачи данных инфраструктуры как услуги	44
	Настройка наборов шифров TLS	47

Проверка безопасности сервера узла	48
Защита ресурсов приложения	48
Обеспечение безопасности узла инфраструктуры как услуги	49

8 Настройка параметров безопасности сети для узла 51

Настройка параметров сети для устройств VMware	51
Заккрытие пользователям доступа к управлению сетевыми интерфейсами	51
Настройка размера очереди невыполненной работы TCP	52
Отклонение эхо-запросов ICMPv4 для получения широковещательного адреса	52
Отключение техники IPv4 Proxy ARP	53
Отклонение сообщений о перенаправлении ICMP IPv4	53
Отклонение ICMP-сообщений о перенаправлении IPv6	54
Регистрация пакетов Martian IPv4	55
Фильтрация обратного тракта IPv4	55
Отклонение переадресации IPv4	56
Отклонение переадресации IPv6	57
Использование Syncookies TCP IPv4	57
Отклонение объявлений маршрутизатора IPv6	58
Отклонение вызовов маршрутизатора IPv6	59
Отклонение предпочтения маршрутизатора IPv6 при вызовах маршрутизатора	59
Отклонение префикса маршрутизатора IPv6	60
Отклонение ограничений прыжков в объявлении маршрутизатора IPv6	61
Отклонение настроек автоматической конфигурации в объявлении маршрутизатора IPv6	62
Отклонение вызовов соседа IPv6	62
Ограничение максимального количества адресов IPv6	63
Настройка параметров сети для узла инфраструктуры как услуги	64
Настройка портов и протоколов	64
Пользовательские порты	65
Порты, необходимые администратору	65

9 Аудит и ведение журнала 69

Безопасная конфигурация

Безопасная конфигурация помогает пользователям оценивать и оптимизировать безопасную конфигурацию развертываний vRealize Automation.

Безопасная конфигурация описывает проверку и настройку безопасных развертываний для типичных сред vRealize Automation и предоставляет сведения и процедуры, которые помогают пользователям делать осознанный выбор, когда речь идет о конфигурации безопасности.

Целевая аудитория

Эти сведения предназначены для системных администраторов и других пользователей vRealize Automation, ответственных за обслуживание и настройку компонентов безопасности системы.

Глоссарий VMware Technical Publications

VMware Technical Publications предоставляет глоссарий с терминами, которые могут быть незнакомы читателю. Определения терминов, используемых в технической документации VMware, можно найти на странице <http://www.vmware.com/support/pubs>.

Обзор базового плана безопасности vRealize Automation

2

VMware предоставляет комплексные рекомендации, чтобы помочь проверить и настроить базовый план безопасности для системы vRealize Automation.

Используйте соответствующие инструменты и процедуры, установленные VMware, для проверки и поддержки безопасной защищенной основной конфигурации для своей системы vRealize Automation. Некоторые компоненты vRealize Automation установлены в защищенном или наполовину защищенном состоянии, но конфигурацию для каждого компонента следует пересмотреть и проверить в свете рекомендаций VMware относительно безопасности, политик безопасности организации и известных угроз.

Состояние безопасности vRealize Automation

Состояние безопасности vRealize Automation предполагает комплексно защищенную среду, основанную на конфигурации системы и сети, корпоративных политиках безопасности, а также рекомендациях по безопасности.

При проверке и настройке усиленной защиты системы vRealize Automation уделите внимание каждой из перечисленных ниже областей, как описано в рекомендациях VMware по усилению защиты.

- Безопасное развертывание
- Безопасная конфигурация
- Безопасность сети

Чтобы убедиться, что система надежно защищена, примите во внимание рекомендации VMware и локальные политики безопасности, так как они относятся к каждой из этих концептуальных областей.

Компоненты системы

При проверке усиленной защиты и безопасной конфигурации системы vRealize Automation убедитесь, что понимаете все компоненты и принципы их совместной работы, обеспечивающей функциональность системы.

Обратите внимание на следующие компоненты при планировании и реализации защищенной системы.

- Устройство vRealize Automation
- Компонент инфраструктуры как услуги

Чтобы поближе познакомиться с решением vRealize Automation и узнать о принципах совместной работы его компонентов, см. раздел *Принципы и понятия* в центре документации VMware vRealize Automation. Сведения о стандартных развертываниях и архитектуре vRealize Automation см. в разделе *Эталонная архитектура*.

Проверка целостности установочного носителя

3

Пользователи всегда должны проверять целостность установочного носителя перед установкой продукта VMware.

Всегда проверяйте хэш SHA1 после скачивания ISO, автономного пакета или исправления, чтобы убедиться в целостности и подлинности скачиваемых файлов. В случае приобретения физического носителя у VMware, если защитная печать повреждена, верните программное обеспечение VMware, чтобы получить замену.

После скачивания носителя воспользуйтесь значением суммы MD5/SHA1, чтобы проверить целостность скачанных файлов. Сравните результат хэша MD5/SHA1 со значением, опубликованным на веб-сайте VMware. Значения хэша SHA1 или MD5 должны совпадать.

Дополнительные сведения о проверке целостности установочного носителя см. на веб-странице <http://kb.vmware.com/kb/1537>.

Усиление защиты инфраструктуры программного обеспечения системы VMware

4

В процессе усиления защиты оцените инфраструктуру развернутого программного обеспечения, которое поддерживает используемую систему VMware, и убедитесь, что она соответствует рекомендациям по защите VMware.

Перед усилением защиты системы VMware проверьте и устраните все недочеты безопасности в инфраструктуре поддерживающего программного обеспечения, чтобы создать полностью защищенную и безопасную среду. Элементы инфраструктуры программного обеспечения, которые следует проверить, включают в себя компоненты операционной системы, поддерживающее программное обеспечение и программное обеспечение базы данных. Устраните недочеты безопасности в этих и других компонентах в соответствии с рекомендациями производителя и другими соответствующими протоколами безопасности.

В эту главу входят следующие разделы:

- Усиление защиты среды VMware vSphere ®
- Усиление защиты узла инфраструктуры как услуги
- Усиление защиты Microsoft SQL Server
- Усиление защиты Microsoft .NET
- Усиление защиты Microsoft Internet Information Services (IIS)

Усиление защиты среды VMware vSphere ®

Оцените среду VMware vSphere ® и убедитесь, что установлен и поддерживается соответствующий уровень требований к защите vSphere.

Дополнительные рекомендации об усилении защиты см. по адресу <http://www.vmware.com/security/hardening-guides.html>.

Инфраструктура VMware vSphere ® является частью среды с комплексной защитой и поэтому должна соответствовать требованиям руководств по безопасности, установленным VMware.

Усиление защиты узла инфраструктуры как услуги

Убедитесь, что защита компьютера с Microsoft Windows, на котором находится узел инфраструктуры как услуги, усилена в соответствии с рекомендациями VMware.

Ознакомьтесь с рекомендациями в соответствующих руководствах Microsoft Windows по усилению защиты и безопасности и убедитесь, что узел Windows Server защищен надлежащим образом. Игнорирование рекомендаций по усилению защиты может привести к тому, что из-за незащищенных компонентов, входящих в выпуски Windows, в системе появятся известные уязвимости безопасности.

Чтобы убедиться, что используемая версия поддерживается, сверьтесь с [Матрицей поддержки vRealize Automation](#).

Обратитесь к поставщику Microsoft, чтобы получить правильные рекомендации по усилению защиты для продуктов Microsoft.

Усиление защиты Microsoft SQL Server

Убедитесь, что база данных Microsoft SQL Server отвечает правилам безопасности, установленным корпорацией Microsoft и VMware.

Ознакомьтесь с рекомендациями в соответствующих руководствах по усилению защиты и безопасности Microsoft SQL Server. Ознакомьтесь со всеми бюллетенями Microsoft по безопасности, касающимися установленной версии Microsoft SQL Server. Игнорирование рекомендаций по усилению защиты может привести к тому, что из-за незащищенных компонентов, входящих в состав версий Microsoft SQL Server, в системе появятся известные уязвимости безопасности.

Чтобы убедиться, что используемая версия Microsoft SQL Server поддерживается, сверьтесь с [Матрицей поддержки vRealize Automation](#).

Обратитесь к поставщику Microsoft, чтобы получить рекомендации по усилению защиты для продуктов Microsoft.

Усиление защиты Microsoft .NET

Платформа Microsoft .NET является частью среды с комплексной защитой и поэтому должна отвечать требованиям руководств по безопасности, установленным Microsoft и VMware.

Ознакомьтесь с рекомендациями, изложенными в соответствующих руководствах по усилению защиты и безопасности .NET. Ознакомьтесь со всеми бюллетенями Microsoft по безопасности, касающимися используемой версии Microsoft SQL Server. Игнорирование рекомендаций по усилению защиты может привести к тому, что из-за незащищенных компонентов, входящих в Microsoft.NET, в системе появятся известные уязвимости безопасности.

Чтобы убедиться, что используемая версия Microsoft.NET поддерживается, сверьтесь с [Матрицей поддержки vRealize Automation](#).

Обратитесь к поставщику Microsoft, чтобы получить рекомендации по усилению защиты для продуктов Microsoft.

Усиление защиты Microsoft Internet Information Services (IIS)

Убедитесь, что службы Microsoft Internet Information Services (IIS) отвечают всем требованиям руководств по безопасности, установленным Microsoft и VMware.

Ознакомьтесь с рекомендациями, изложенными в соответствующих руководствах по усилению защиты и безопасности Microsoft IIS. Изучите также все бюллетени Microsoft по безопасности, касающиеся используемой версии IIS. Игнорирование рекомендаций по усилению защиты может привести к тому, что в системе появятся известные уязвимости безопасности.

Чтобы убедиться, что используемая версия поддерживается, сверьтесь с [Матрицей поддержки vRealize Automation](#).

Обратитесь к поставщику Microsoft, чтобы получить рекомендации по усилению защиты для продуктов Microsoft.

Проверка установленного программного обеспечения

5

Так как уязвимости в стороннем и неиспользуемом программном обеспечении повышают риск несанкционированного доступа к системе и нарушения доступности, важно проверить все программное обеспечение, установленное на компьютерах узлов VMware, и оценить его использование.

Не устанавливайте программное обеспечение, которое не требуется для безопасной работы системы на компьютерах узлов VMware. Удалите неиспользуемое или лишнее программное обеспечение.

Инвентаризация установленного неподдерживаемого программного обеспечения

Оцените свое развертывание VMware и выполните инвентаризацию установленных продуктов, чтобы убедиться, что не установлено ни одной лишней неподдерживаемой программы.

Дополнительные сведения о политиках поддержки сторонних продуктов см. в статье о поддержке VMware по адресу <https://www.vmware.com/support/policies/thirdparty.html>.

Проверка стороннего программного обеспечения

VMware не поддерживает и не рекомендует установку стороннего программного обеспечения, которое не было протестировано и проверено. небезопасное, неисправленное или не прошедшее проверку подлинности стороннее программное обеспечение, установленное на компьютерах узлов VMware, может подвергнуть систему риску несанкционированного доступа и нарушения доступности. При необходимости использовать неподдерживаемое стороннее программное обеспечение посоветуйтесь со сторонним поставщиком по поводу требований к безопасной конфигурации и исправлению.

Инструкции и исправления для системы безопасности VMware

6

Для поддержания максимального уровня защиты ваших систем следуйте инструкциям по безопасности VMware и применяйте все соответствующие исправления.

VMware выпускает инструкции по безопасности для продуктов. Следите за обновлениями этих инструкций, и обеспечивайте защиту используемых продуктов от известных угроз.

Оцените журналы установки vRealize Automation, исправлений и обновлений, а также убедитесь, что выпущенные инструкции по безопасности VMware применены и соблюдаются.

Дополнительные сведения о текущих инструкциях по безопасности VMware см. на веб-странице <http://www.vmware.com/security/advisories/>.

Безопасная конфигурация

Проверьте и обновите параметры безопасности для виртуальных устройств vRealize Automation и компонента инфраструктуры как услуги в соответствии с конфигурацией своей системы. Кроме того, проверьте и обновите конфигурацию других компонентов и приложений.

Безопасная настройка установки vRealize Automation включает в себя индивидуальную настройку всех компонентов и их совместной работы. Продумайте конфигурацию всех системных компонентов во взаимодействии, чтобы достичь приемлемого уровня безопасности.

В эту главу входят следующие разделы:

- [Обеспечение безопасности устройства vRealize Automation](#)
- [Защита компонента инфраструктуры как услуги](#)

Обеспечение безопасности устройства vRealize Automation

Проверьте и обновите настройки безопасности для устройства vRealize Automation в соответствии с конфигурацией системы.

Настройте параметры безопасности для виртуальных устройств и операционных систем соответствующих узлов. Также настройте или подтвердите конфигурацию других связанных компонентов и приложений. В одних случаях для достижения необходимой конфигурации требуется подтвердить текущие настройки, в других — изменить или добавить какие-либо настройки.

Изменение пароля пользователя root

Можно изменить пароль пользователя root для устройства vRealize Automation.

Процедура

1. Выполните вход в интерфейс управления устройства vRealize Automation как пользователь root.
`https://vrealize-automation-appliance-FQDN:5480`
2. Откройте вкладку **Администратор**.
3. Щелкните подменю **Администрирование**.
4. Введите текущий пароль в текстовом поле **Текущий пароль администратора**.
5. Введите новый пароль в текстовом поле **Новый пароль администратора**.
6. Введите новый пароль в текстовом поле **Повторный ввод нового пароля администратора**.

7. Нажмите кнопку **Сохранить настройки**.

Проверка сложности и хэша пароля пользователя **Root**

Пароль пользователя **root** должен соответствовать корпоративным требованиям к сложности паролей в вашей организации.

Подтверждение сложности пароля пользователя **root** требуется, когда пользователь **root** проходит проверку сложности пароля к модулю **pam_cracklib** , который применяется к учетным записям пользователя.

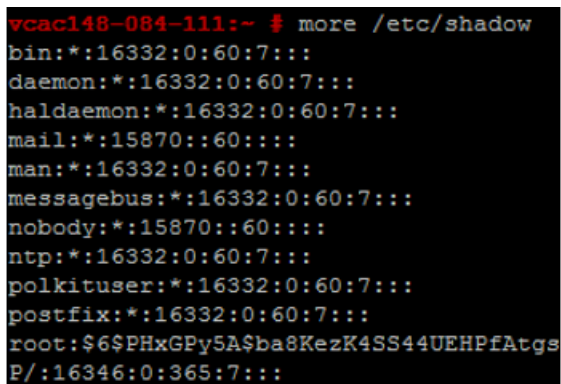
Пароль к учетной записи должен начинаться с **\$6\$**, что указывает на хэш **sha512**. Это стандартный хэш для всех устройств с аппаратной защитой.

Процедура

1. Чтобы подтвердить хэш пароля пользователя **root**, войдите как пользователь **root** и запустите команду **# more /etc/shadow**.

Отобразятся сведения хэша.

Рис. 7-1. Результаты хэша пароля



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPY5A$ba8KzK4SS44UEHPfAtgs
P/:16346:0:365:7:::
```

2. Если пароль пользователя **root** не содержит хэш **sha512**, запустите команду **passwd**, чтобы изменить его.

Для всех устройств с аппаратной защитой используется **enforce_for_root** для модуля **pw_history**, который находится в файле **etc/pam.d/common-password**. Система по умолчанию запоминает пять последних паролей. Старые пароли хранятся для каждого пользователя в файле **/etc/securetty/passwd**.

Проверка журнала паролей пользователей **root**

Убедитесь, что журнал паролей применен для учетной записи пользователя **root**.

Для всех устройств с аппаратной защитой используется **enforce_for_root** для модуля **pw_history**, который находится в файле **etc/pam.d/common-password**. Система по умолчанию запоминает пять последних паролей. Старые пароли хранятся для каждого пользователя в файле **/etc/securetty/passwd**.

Процедура

1. Выполните следующую команду:

```
cat /etc/pam.d/common-password-vmware.local | grep pam_pwhistory.so
```

2. Убедитесь, что `enforce_for_root` отображается в возвращенных результатах.

```
password required pam_pwhistory.so enforce_for_root remember=5 retry=3
```

Управление сроком действия пароля

Настройте срок действия пароля для всех учетных записей в соответствии с политиками безопасности организации.

По умолчанию во всех учетных записях виртуального устройства VMware с усиленной защитой используется 60-дневный срок действия пароля. На большинстве защищенных устройств для учетной записи пользователя `root` установлен 365-дневный срок действия пароля. Рекомендуется убедиться, что срок действия во всех учетных записях соответствует требованиям стандартов безопасности и эксплуатации.

Если срок действия пароля пользователя `root` истекает, его нельзя возобновить. Чтобы предотвратить истечение срока действия паролей администратора и пользователя `root`, необходимо применить политики, действующие на конкретном объекте.

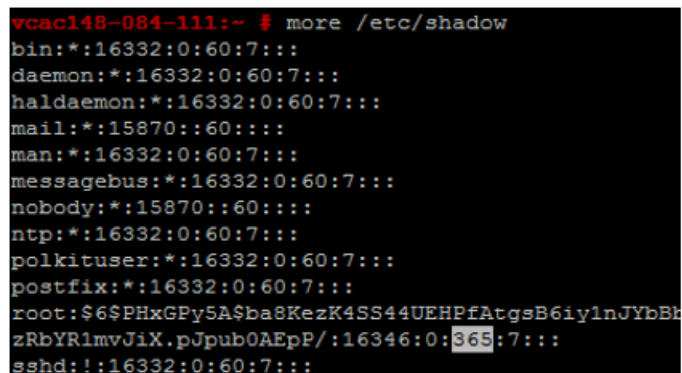
Процедура

1. Войдите в компьютеры виртуального устройства как пользователь `root` и выполните следующую команду, чтобы проверить срок действия пароля во всех учетных записях.

```
# cat /etc/shadow
```

Срок действия пароля — это пятое поле (поля разделяются двоеточиями) теневого файла. Срок действия пароля пользователя `root` задается в днях.

Рис. 7-2. Поле «Срок действия пароля»



```
vcac148-084-111:~ # more /etc/shadow
bin:!:16332:0:60:7:::
daemon:!:16332:0:60:7:::
haldaemon:!:16332:0:60:7:::
mail:!:15870::60:::
man:!:16332:0:60:7:::
messagebus:!:16332:0:60:7:::
nobody:!:15870::60:::
ntp:!:16332:0:60:7:::
polkituser:!:16332:0:60:7:::
postfix:!:16332:0:60:7:::
root:$6$PHxGPy5A$ba8KezK4SS44UEHPfAtgsB6iy1nJYbBkzRbYR1mvJiX.pJpub0AEpP/:16346:0:365:7:::
sshd:!:16332:0:60:7:::
```

2. Чтобы изменить срок действия учетной записи пользователь `root`, выполните команду следующей формы.

```
# passwd -x 365 root
```


В этой команде число 365 указывает на количество дней до окончания срока действия пароля.

Используйте ту же команду, чтобы изменить любого пользователя, заменив определенную учетную запись пользователем **root** и заменив количество дней для соответствия стандартам организации в отношении срока действия.

Управление учетными записями SSH и администратора

Для удаленных соединений все устройства с усиленной защитой включают протокол безопасной оболочки (SSH). Используйте протокол SSH при необходимости и управляйте им надлежащим образом, чтобы сохранить безопасность системы.

SSH — это интерактивная среда командной строки, которая поддерживает удаленные подключения к виртуальным устройствам VMware. По умолчанию для доступа к SSH требуются учетные данные учетной записи пользователя с высоким уровнем привилегий. Действия пользователя **root** с SSH обычно обходят контроль доступа на основе ролей (RBAC) и элементы управления аудитом виртуальных устройств.

Рекомендуется отключить SSH в производственной среде и активировать этот протокол только для устранения проблем, которые не удастся решить другими средствами. Оставляйте его включенным, только если он требуется для конкретной цели, и делайте это в соответствии с политиками безопасности своей организации. По умолчанию протокол SSH отключен на устройстве vRealize Automation. В зависимости от конфигурации vSphere можно включить или отключить протокол SSH при развертывании шаблона Open Virtualization Format (OVF).

В качестве простого теста для определения того, включен ли протокол SSH на компьютере, попытайтесь открыть подключение с помощью SSH. Если подключение открывается и запрашивает учетные данные, протокол SSH включен и доступен для подключений.

Учетная запись пользователя **root** SSH

Устройства VMware не включают предварительно настроенные учетные записи пользователей, поэтому учетная запись пользователя **root** может по умолчанию использовать протокол SSH, чтобы входить напрямую. Войдите как пользователь **root** и отключите протокол SSH как можно скорее.

Чтобы выполнять требования нормативно-правовых стандартов в отношении невозможности отказа, на всех защищенных устройствах сервер SSH предварительно настроен с помощью записи **wheel AllowGroups** на то, чтобы доступ к SSH могла получать только вспомогательная группа **wheel**. С целью разделения обязанностей можно изменить запись **wheel AllowGroups** в файле **/etc/ssh/sshd_config** для использования другой группы, например **sshd**.

Группа **wheel** может использовать модуль **pat_wheel** для суперпользовательского доступа, поэтому ее члены могут выполнять функции пользователя **root**, для которых требуется его пароль. Разделение групп дает возможность пользователям использовать SSH для подключения к устройству, но не выполнять функции пользователя **root**. Не удаляйте и не изменяйте другие записи в поле **AllowGroups**, которое обеспечивает правильную работу устройства. После внесения изменения необходимо перезагрузить управляющую программу SSH, выполнив команду: **# service sshd restart**.

Включение и выключение SSH на устройствах vRealize Automation

Протокол безопасной оболочки (SSH) на устройстве vRealize Automation следует включать только для устранения неполадок. Во время обычной работы на этапе производства протокол SSH должен быть выключен в этих компонентах.

Включить и выключить протокол SSH на устройстве vRealize Automation можно с помощью интерфейса управления устройством vRealize Automation.

Процедура

1. Выполните вход в интерфейс управления устройством vRealize Automation как пользователь **root**.
`https://vrealize-automation-appliance-FQDN:5480`
2. Откройте вкладку **Администратор**.
3. Откройте подменю **Администратор**.
4. Установите флажок **Включить службу SSH**, чтобы включить SSH, или снимите этот флажок, чтобы выключить SSH.
5. Щелкните элемент **Сохранить настройки**, чтобы сохранить изменения.

Создание локальной учетной записи администратора для SSH

В целях безопасности рекомендуется создать и настроить на узлах виртуального устройства локальные учетные записи администратора для безопасной оболочки (протокол SSH). После создания этих учетных записей следует удалить доступ пользователя **root** к SSH.

Создайте учетные записи администратора для SSH или участников второстепенной группы **wheel**, либо и то и другое. Прежде чем отключить прямой доступ пользователя **root**, протестируйте доступ авторизованных администраторов к SSH с помощью параметра **AllowGroups** и убедитесь, что они могут использовать команду **su to root** с помощью группы **wheel**.

Процедура

1. Выполните вход на виртуальном устройстве в качестве пользователя **root** и запустите указанные ниже команды с соответствующими именами пользователя.

```
# useradd -g users <username> -G wheel -m -d /home/имя_пользователя
# passwd username
```

«Wheel» — группа, указанная в параметре **AllowGroups** для доступа к SSH. Для добавления нескольких второстепенных групп используйте команду `-G wheel,sshd`.

2. Переключитесь на профиль пользователя и укажите новый пароль, чтобы повысить сложность пароля и надежность его проверки.

```
# su -username
# username@hostname:~>passwd
```

Если требования к сложности пароля выполнены, пароль будет обновлен. В противном случае восстановится исходный пароль и вам необходимо будет запустить команду пароля заново.

3. Чтобы отменить прямой вход в SSH, замените запись `(#)PermitRootLogin yes` на `PermitRootLogin no` в файле `/etc/ssh/sshd_config`.

Вы также можете включить или выключить SSH в интерфейсе управления виртуального устройства, установив или сняв флажок **Вход администратора в SSH включен** на вкладке **Администрирование**.

Следующие шаги

Отключите прямой вход от имени пользователя `root`. По умолчанию на устройствах с повышенной надежностью разрешен прямой доступ к профилю пользователя `root` через консоль. После того как вы создадите учетные записи администратора для предотвращения отказа и проверите их доступ `su-root` с помощью группы `wheel`, отключите прямой вход пользователя `root`, заменив от имени пользователя `root` запись `tty1` на `console` в файле `/etc/security`.

1. Откройте файл `/etc/securetty` в текстовом редакторе.
2. Найдите запись `tty1` и замените ее на `console`.
3. Сохраните файл и закройте его.

Повышение надежности конфигурации SSH-сервера

Все устройства VMware по умолчанию имеют конфигурацию с повышенной надежностью (если это возможно). Уровень надежности конфигурации можно проверить, просмотрев настройки служб сервера и клиента в разделе глобальных параметров в файле конфигурации.

Процедура

1. Откройте файл конфигурации сервера `/etc/ssh/sshd_config` на устройстве VMware и проверьте правильность настроек.

Параметр	Состояние
Протокол управляющей программы сервера	Протокол 2
Шифры CBC	aes256-ctr и aes128-ctr
Переадресация TCP	AllowTCPForwarding: нет
Порты шлюзов сервера	Порты шлюзов: нет
Переадресация X11	X11Forwarding: нет
Служба SSH	Используйте поле <code>AllowGroups</code> и определите разрешенный доступ для группы. Добавьте в группу соответствующих участников.
Проверка подлинности GSSAPI	GSSAPIAuthentication: нет, если не используется
Проверка подлинности Kerberos	KerberosAuthentication: нет, если не используется
Локальные переменные (глобальный параметр <code>AcceptEnv</code>)	Установите значение отключено комментированием или включено для переменных <code>LC_*</code> или <code>LANG</code>
Конфигурация туннеля	PermitTunnel: нет

Параметр	Состояние
Сетевые сеансы	MaxSessions: 1
Одновременные соединения пользователя	Установите значение 1 для пользователя root и любого другого пользователя. Для файла /etc/security/limits.conf требуется такая же настройка.
Проверка в строгом режиме	Строгие режимы: да
Разделение привилегий	UsePrivilegeSeparation: да
Проверка подлинности RSA файла .rhosts	RhostsESAAuthentication: нет
Сжатие	Сжатие: отложено или отсутствует
Код проверки подлинности сообщения	MACs hmac-sha1
Ограничение доступа пользователя	PermitUserEnvironment: нет

2. Сохраните изменения и закройте файл.

Повышение надежности конфигурации SSH-клиента

В рамках повышения надежности системы следует проверить надежность SSH-клиента. Для этого необходимо убедиться, что файл конфигурации SSH-клиента на узлах виртуального устройства настроен в соответствии с инструкциями VMware.

Процедура

1. Откройте файл конфигурации SSH-клиента (/etc/ssh/ssh_config) и проверьте правильность настроек в разделе глобальных параметров.

Параметр	Состояние
Протокол клиента	Протокол 2
Порты шлюзов клиента	Порты шлюзов: нет
Проверка подлинности GSSAPI	GSSAPIAuthentication: нет
Локальные переменные (глобальный параметр SendEnv)	Укажите только переменные LC_* или LANG
Шифры CBC	Только aes256-ctr и aes128-ctr
Коды проверки подлинности сообщения	Используется только в записи MACs hmac-sha1

2. Сохраните изменения и закройте файл.

Проверка разрешений файла ключа SSH

Чтобы свести к минимуму вероятность вредоносных атак, поддерживайте критически важные разрешения файла ключа SSH на компьютерах узла виртуальных устройств.

После настройки или обновления конфигурации SSH всегда проверяйте, не изменились ли следующие разрешения файла ключа SSH.

- Файлы ключа общедоступного узла, расположенные в каталоге `/etc/ssh/*key.pub`, принадлежат пользователю `root` и устанавливают для разрешений значение «0644» (`-rw-r--r--`).
- Файлы ключа частного узла, расположенные в каталоге `/etc/ssh/*key`, принадлежат пользователю `root` и устанавливают для разрешений значение «0600» (`-rw-----`).

Проверка разрешений для файла SSH-ключей

Убедитесь, что разрешения SSH применяются к файлам открытых и закрытых ключей.

Процедура

1. Проверьте файлы открытых SSH-ключей с помощью следующей команды: `ls -l /etc/ssh/*key.pub`
2. Убедитесь, что владелец — `root`, что владелец группы — `root`, и что для файлов установлены разрешения 0644 (`-rw-r--r--`).
3. Устраните любые проблемы с помощью следующих команд.

```
chown root /etc/ssh/*key.pub
```

```
chgrp root /etc/ssh/*key.pub
```

```
chmod 644 /etc/ssh/*key.pub
```

4. Проверьте файлы закрытых SSH-ключей с помощью следующей команды: `ls -l /etc/ssh/*key`
5. Убедитесь, что владельцем является пользователь `root`, владельцем группы также является `root`, а для файлов установлены разрешения с кодом 0600 (`-rw-----`). Устраните любые проблемы с помощью следующих команд.

```
chown root /etc/ssh/*key
```

```
chgrp root /etc/ssh/*key
```

```
chmod 600 /etc/ssh/*key
```

Изменение пользователей в интерфейсе управления виртуального устройства

Чтобы обеспечить требуемый уровень безопасности, можно добавлять и удалять пользователей в интерфейсе управления виртуального устройства.

Учетная запись пользователя `root` для интерфейса управления виртуального устройства использует PAM для проверки подлинности. Таким образом, будут применяться также уровни обрезки, заданные PAM. Если интерфейс управления виртуального устройства не был изолирован надлежащим образом, возможна блокировка системной учетной записи пользователя `root` в случае, если эта учетная запись стала объектом атаки методом перебора. Кроме того, если прав пользователя `root` недостаточно для обеспечения неподдельности для нескольких пользователей в организации, рекомендуется изменить администратора для интерфейса управления.

Необходимые условия

Процедура

1. Выполните следующую команду, чтобы создать нового пользователя и добавить его в группу интерфейса управления виртуального устройства.

```
useradd -G vami,root пользователь
```

2. Создайте пароль для учетной записи пользователя.

```
passwd пользователь
```

3. (дополнительно) Выполните следующую команду, чтобы запретить доступ пользователя `root` к интерфейсу управления виртуального устройства.

```
usermod -R vami root
```

Примечание При запрете доступа пользователя `root` к интерфейсу управления виртуального устройства будет также отключена функция обновления пароля администратора или пользователя `root` на вкладке «Администратор».

Настройка проверки подлинности загрузчика

Чтобы обеспечить необходимый уровень защиты, настройте проверку подлинности загрузчика на виртуальных устройствах VMware.

Если загрузчику системы не требуется проверка подлинности, пользователи с доступом к консоли системы могут изменять конфигурацию загрузки системы или загружать систему в однопользовательском режиме либо режиме обслуживания, что может привести к отказу в обслуживании или несанкционированному доступу к системе. Проверка подлинности загрузчика не задана по умолчанию на виртуальных устройствах VMware, поэтому необходимо создать пароль GRUB, чтобы настроить ее.

Процедура

1. Убедитесь, что пароль загрузки существует. Для этого найдите строку `password --md5 <password-hash>` в файле `/boot/grub/menu.lst` на виртуальных устройствах.

2. Если пароля не существует, выполните команду `# /usr/sbin/grub-md5-crypt` на виртуальном устройстве.

Будет создан пароль MD5, и команда предоставит выходные данные хэша md5.

3. Добавьте пароль в файл `menu.lst`, выполнив команду `# password --md5 <hash from grub-md5-crypt>`.

Настройка NTP

Если источники времени имеют критически важное значение, отключите синхронизацию времени узлов и используйте на устройстве vRealize Automation протокол NTP (Network Time Protocol).

Управляющая программа NTP на устройстве vRealize Automation обеспечивает синхронизированную работу служб времени. По умолчанию протокол NTP отключен, поэтому его необходимо настроить вручную. Если это возможно, используйте протокол NTP в производственных средах — это позволит отслеживать действия пользователей и выявлять потенциально опасные атаки и вторжения посредством надлежащего аудита и ведения журнала. Уведомления о безопасности NTP см. на веб-сайте NTP.

Файл конфигурации NTP находится в папке `/etc/` на каждом устройстве. Вы можете включить службу NTP для устройства vRealize Automation и добавить серверы времени на вкладке **Администрирование** в интерфейсе управления виртуального устройства.

Процедура

1. С помощью текстового редактора откройте файл конфигурации `/etc/ntp.conf` на компьютере узлов виртуального устройства.
2. В качестве владельца файла укажите **root:root**.
3. В качестве разрешений укажите **0640**.
4. Чтобы снизить риск атак типа «отказ в обслуживании» с лавинообразным умножением данных в отношении службы NTP, откройте файл `/etc/ntp.conf` и убедитесь, что в нем есть строки ограничений.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

5. Сохраните изменения и закройте файлы.

Настройка TLS для передачи данных устройства vRealize Automation

В развертывании vRealize Automation должны использоваться надежные протоколы TLS в целях защиты каналов передачи для компонентов устройства vRealize Automation.

В целях повышения производительности протокол TLS не включен для передачи данных между некоторыми службами приложений на локальных узлах. Если требуется многослойная система защиты, включите TLS для всех случаев передачи данных на локальных узлах.

Важно! Если действие TLS завершается на подсистеме балансировки нагрузки, отключите ненадежные протоколы, например SSLv2, SSLv3 и TLS 1.0, на всех подсистемах балансировки нагрузки.

Включение TLS в конфигурации локального узла

По умолчанию TLS не используется для передачи данных на некоторых локальных узлах. TLS можно включить для передачи данных на всех локальных узлах, чтобы повысить уровень безопасности.

Процедура

1. Подключитесь к Устройство vRealize Automation с помощью SSH.

2. Установите разрешения для хранилища ключей `vcac`, выполнив указанные далее команды.

```
usermod -A vco,coredump,pivotal vco
chown vcac.pivotal /etc/vcac/vcac.keystore
chmod 640 /etc/vcac/vcac.keystore
```

3. Обновите конфигурацию `HAProxy`.

- а) Откройте файл конфигурации `HAProxy`, расположенный в папке `/etc/haproxy/conf.d`, и выберите службу `20-vcac.cfg`.

- б) Найдите строки, содержащие:

`server local 127.0.0.1...` и добавьте в конце них: `ssl verify none`

В данном разделе содержатся другие строки, например:

```
backend-horizon      backend-vro
backend-vra          backend-artifactory
backend-vra-health
```

- в) Измените порт для `backend-horizon` с `8080` на `8443`.

4. Получите пароль `keystorePass`.

- а) Найдите свойство `certificate.store.password` в файле `/etc/vcac/security.properties`.

Например, `certificate.store.password=s2enc~iom0GXATG+RB8ff7Wdm4Bg==`.

- б) Опишите значение с помощью следующей команды:

```
vcac-config prop-util -d --p VALUE
```

Например, `vcac-config prop-util -d --p s2enc~iom0GXATG+RB8ff7Wdm4Bg==`.

5. Настройте службу `vRealize Automation`.

- а) Откройте файл `/etc/vcac/server.xml`.

- б) Добавьте указанный ниже атрибут в тег «Соединитель», заменив `certificate.store.password` на пароль хранилища сертификатов, значение которого указано в `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/
vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```

6. Настройте службу `vRealize Orchestrator`.

- а) Откройте файл `/etc/vco/app-server.xml`

- б) Добавьте указанный ниже атрибут в тег «Соединитель», заменив `certificate.store.password` на пароль хранилища сертификатов, значение которого указано в `etc/vcac/security.properties`.

```
scheme="https" secure="true" SSLEnabled="true" sslProtocol="TLS" keystoreFile="/etc/vcac/
vcac.keystore" keyAlias="apache" keystorePass="certificate.store.password"
```


7. Перезапустите службы vRealize Orchestrator, vRealize Automation и HAProxy.

```
service vcac-server restart
service vco-server restart
service haproxy restart
```

Примечание Если сервер VCO не перезапускается, перезагрузите главный компьютер.

8. Настройте интерфейс управления виртуального устройства.

Чтобы просмотреть состояние служб, выполните следующую команду на виртуальном устройстве vRealize Automation.

```
curl -ks -H "Content-Type: application/json" https://localhost/component-registry/services/status/
current?limit=200 | jq -re '.content[]|"\(.serviceStatus.serviceName) \
(.serviceStatus.serviceInitializationStatus)'"'
```

Примечание Если включить протокол SSL в интерфейсе управления виртуальными устройствами, на вкладке «Службы» нельзя будет просмотреть состояние служб vRealize Automation.

- а) Откройте файл /opt/vmware/share/htdocs/service/café-services/services.py.
- б) Измените строку `conn = httplib.HTTP()` на `conn = httplib.HTTPS()` для повышения уровня безопасности.

Включение режима соответствия федеральному стандарту обработки информации (Federal Information Processing Standard, FIPS) 140-2

На устройстве vRealize Automation сейчас используется версия OpenSSL, соответствующая стандарту FIPS 140-2, для передачи данных через TLS в рамках любого входящего и исходящего сетевого трафика.

Включить и выключить режим FIPS можно в интерфейсе управления устройства vRealize Automation. Можно также настроить режим FIPS с помощью командной строки, войдя в систему как пользователь `root` и выполнив одну из следующих команд:

```
vcac-vami fips enable
vcac-vami fips disable
vcac-vami fips status
```

Если включен режим FIPS, для входящего и исходящего сетевого трафика устройства vRealize Automation порта 443 используется шифрование по стандарту FIPS 140-2. Независимо от настроек FIPS, в vRealize Automation используется стандарт AES-256 для обеспечения безопасности защищенных данных, которые хранятся на устройстве vRealize Automation.

Примечание В данный момент в vRealize Automation соответствие FIPS обеспечивается лишь частично, так как сертифицированные криптографические модули используются еще не во всех внутренних компонентах. В случаях, когда сертифицированные модули еще не внедрены, во всех криптографических алгоритмах используется шифрование на основе стандарта AES-256.

Примечание Следующая процедура перезагрузит физический компьютер при изменении конфигурации.

Процедура

1. Войдите в интерфейс управления устройства vRealize Automation как пользователь root.
`https://vrealize-automation-appliance-FQDN:5480`
2. Выберите **vRA > Настройки узла**.
3. Нажмите кнопку под заголовком «Действия» справа сверху, чтобы включить или выключить режим FIPS.
4. Нажмите кнопку **Да**, чтобы перезапустить устройство vRealize Automation.

Проверка отключения протоколов SSLv3, TLS 1.0 и TLS 1.1

В целях аппаратной защиты убедитесь, что развернутое устройство Устройство vRealize Automation использует защищенные каналы передачи данных.

Примечание После отключения TLS 1.0/1.1 и включения TLS 1.2 выполнить операцию присоединения к кластеру будет невозможно

Необходимые условия

Выполните [Включение TLS в конфигурации локального узла](#).

Процедура

1. Убедитесь, что SSLv3, TLS 1.0 и TLS 1.1 отключены в https-обработчиках HAProxy устройства Устройство vRealize Automation.

Просмотрите этот файл	Проверьте наличие таких элементов	В соответствующей строке, как показано
/etc/haproxy/conf.d/20-vcac.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11
/etc/haproxy/conf.d/30-vro-config.cfg	no-sslv3 no-tlsv10 no-tls11 force-tls12	bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-sslv3 no-tlsv10 no-tlsv11

2. Перезапустите службу.

```
service haproxy restart
```

3. Откройте файл `/opt/vmware/etc/lighttpd/lighttpd.conf` и убедитесь, что в нем отображаются правильные записи отключения.

Примечание Указания относительно отключения TLS 1.0 или TLS 1.1 на сервере Lighttpd нет. Ограничение использования TLS 1.1 и TLS 1.0 можно частично обойти, запретив OpenSSL использовать наборы шифров TLS 1.0 и TLS 1.1.

```
ssl.use-ssl2 = "disable"
ssl.use-ssl3 = "disable"
```

4. Убедитесь, что протоколы SSLv3, TLS 1.0 и TLS 1.1 отключены для прокси-сервера консоли на Устройство vRealize Automation.
 - а) Отредактируйте файл `/etc/vcac/security.properties`, добавив или изменив следующую строку:


```
consoleproxy.ssl.server.protocols = TLSv1.2
```
 - б) Перезапустите сервер с помощью следующей команды:


```
service vcac-server restart
```
5. Убедитесь, что SSLv3, TLS 1.0 и TLS 1.1 отключены для службы vCO.
 - а) Найдите тег `<Connector>` в файле `/etc/vco/app-server/server.xml` и добавьте следующий атрибут:


```
sslEnabledProtocols = "TLSv1.2"
```
 - б) Перезапустите службу vCO, выполнив следующую команду.


```
service vco-server restart
```
6. Убедитесь, что SSLv3, TLS 1.0 и TLS 1.1 отключены для службы vRealize Automation.
 - а) Добавьте следующие атрибуты к тегу `<Connector>` в файле `/etc/vcac/server.xml`

```
sslEnabledProtocols = "TLSv1.2"
```
 - б) Перезапустите службу vRealize Automation, выполнив следующую команду:


```
service vcac-server restart
```
7. Убедитесь, что SSLv3, TLS 1.0 и TLS 1.1 отключены для RabbitMQ.

Откройте файл `/etc/rabbitmq/rabbitmq.config` и убедитесь, что в разделах `ssl` и `ssl_options` присутствует только `{versions, ['tlsv1.2']}`.

```
[
  {ssl, [
    {versions, ['tlsv1.2']},
    {ciphers, ["AES256-SHA", "AES128-SHA"]}
  ]},
  {rabbit, [
    {tcp_listeners, [{"127.0.0.1", 5672}]},
    {frame_max, 262144},
```

```

    {ssl_listeners, [5671]},
    {ssl_options, [
        {cacertfile, "/etc/rabbitmq/certs/ca/cacert.pem"},
        {certfile, "/etc/rabbitmq/certs/server/cert.pem"},
        {keyfile, "/etc/rabbitmq/certs/server/key.pem"},
        {versions, ['tlsv1.2']},
        {ciphers, ["AES256-SHA", "AES128-SHA"]},
        {verify, verify_peer},
        {fail_if_no_peer_cert, false}
    ]},
    {mnesia_table_loading_timeout, 600000},
    {cluster_partition_handling, autoheal},
    {heartbeat, 600}
  ]},
  {kernel, [{net_ticktime, 120}]}
].

```

8. Перезапустите сервер RabbitMQ.

```
# service rabbitmq-server restart
```

9. Убедитесь, что SSLv3, TLS 1.0 и TLS 1.1 отключены для службы vIDM.

Откройте файл `opt/vmware/horizon/workspace/conf/server.xml` для каждого экземпляра соединителя, который содержит `SSLEnabled="true"`, и убедитесь, что в нем есть следующая строка.

```
ssLEnabledProtocols="TLSv1.2"
```

Настройка наборов шифров TLS для компонентов vRealize Automation

Чтобы обеспечить максимальную безопасность, необходимо настроить для компонентов vRealize Automation использование криптостойких шифров.

Шифр, согласованный между сервером и браузером, определяет надежность шифрования для TLS-сеанса.

Чтобы всегда использовались только криптостойкие шифры, отключите легко раскрываемые шифры в компонентах vRealize Automation. Настройте для сервера поддержку только криптостойких шифров и использование ключей достаточно большого размера. Также следует настроить надлежащий порядок для всех шифров.

Отключите наборы шифров, которые не обеспечивают проверку подлинности, например наборы шифров NULL, aNULL, eNULL. Также отключите анонимный обмен ключами по протоколу Диффи-Хеллмана (ADH), шифры экспортного уровня (EXP, шифры, содержащие DES), ключи размером менее 128 бит для шифрования полезной нагрузки, использование MD5 в качестве механизма хэширования для полезной нагрузки, наборы шифров IDEA и RC4. Убедитесь также, что выключены наборы шифров, для которых используется обмен ключами по протоколу Диффи-Хеллмана (DHE).

Отключение легко раскрываемых шифров в HA Proxy

Сравните шифры службы HA Proxy устройства vRealize Automation со списком допустимых шифров и отключите все те из них, которые считаются легко раскрываемыми.

Отключите наборы шифров, которые не обеспечивают проверку подлинности, например наборы шифров NULL, aNULL, eNULL. Также отключите анонимный обмен ключами по протоколу Диффи-Хеллмана (ADH), шифры экспортного уровня (EXP, шифры, содержащие DES), ключи размером менее 128 бит для шифрования полезной нагрузки, использование MD5 в качестве механизма хэширования для полезной нагрузки, наборы шифров IDEA и RC4.

Процедура

1. Просмотрите шифры в файле `/etc/haproxy/conf.d/20-vcac.cfg` для директивы привязки и отключите все те, которые считаются легко раскрываемыми.

```
bind 0.0.0.0:443 ssl crt /etc/apache2/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

2. Просмотрите шифры в файле `/etc/haproxy/conf.d/30-vro-config.cfg` для директивы привязки и отключите все те, которые считаются легко раскрываемыми.

```
bind :::8283 v4v6 ssl crt /opt/vmware/etc/lighttpd/server.pem ciphers !aNULL:!eNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH no-ssl3 no-tls10 no-tls11
```

Отключение легко раскрываемых шифров в службе прокси-сервера консоли на устройстве **Устройство vRealize Automation**

Сравните шифры службы прокси-сервера консоли на устройстве vRealize Automation со списком допустимых шифров и отключите все те из них, которые считаются легко раскрываемыми.

Отключите наборы шифров, которые не обеспечивают проверку подлинности, например наборы шифров NULL, aNULL, eNULL. Также отключите анонимный обмен ключами по протоколу Диффи-Хеллмана (ADH), шифры экспортного уровня (EXP, шифры, содержащие DES), ключи размером менее 128 бит для шифрования полезной нагрузки, использование MD5 в качестве механизма хэширования для полезной нагрузки, наборы шифров IDEA и RC4.

Процедура

1. Откройте в текстовом редакторе файл `/etc/vcac/security.properties`.
2. Добавьте в файл строку, чтобы отключить ненужные наборы шифров.

Строка должна выглядеть так:

```
consoleproxy.ssl.ciphers.disallowed=cipher_suite_1, cipher_suite_2, и т. д.
```

Например, чтобы отключить наборы шифров AES 128 и AES 256, используйте следующую строку:

```
consoleproxy.ssl.ciphers.disallowed=TLS_DH_DSS_WITH_AES_128_CBC_SHA,
TLS_DH_DSS_WITH_AES_256_CBC_SHA, TLS_DH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

3. Перезапустите сервер с помощью следующей команды:

```
service vcac-server restart
```

Отключение легко раскрываемых шифров в службе vCO Устройство vRealize Automation

Сравните шифры службы vCO Устройство vRealize Automation со списком допустимых шифров и отключите все те из них, которые считаются легко раскрываемыми.

Отключите наборы шифров, которые не обеспечивают проверку подлинности, например наборы шифров NULL, aNULL, eNULL. Также отключите анонимный обмен ключами по протоколу Диффи-Хеллмана (ADH), шифры экспортного уровня (EXP, шифры, содержащие DES), ключи размером менее 128 бит для шифрования полезной нагрузки, использование MD5 в качестве механизма хэширования для полезной нагрузки, наборы шифров IDEA и RC4.

Процедура

1. Найдите в файле `/etc/vco/app-server/server.xml` тег `<Connector>`.
2. Измените или добавьте атрибут шифра, чтобы применить необходимые наборы шифров.

Пример:

```
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

Отключение легко раскрываемых шифров в службе RabbitMQ Устройство vRealize Automation

Сравните шифры службы RabbitMQ Устройство vRealize Automation со списком допустимых шифров и отключите те из них, которые считаются легко раскрываемыми.

Отключите наборы шифров, которые не обеспечивают проверку подлинности, например наборы шифров NULL, aNULL, eNULL. Также отключите анонимный обмен ключами по протоколу Диффи-Хеллмана (ADH), шифры экспортного уровня (EXP, шифры, содержащие DES), ключи размером менее 128 бит для шифрования полезной нагрузки, использование MD5 в качестве механизма хэширования для полезной нагрузки, наборы шифров IDEA и RC4.

Процедура

1. Проверьте поддерживаемые наборы шифров с помощью команды `# /usr/sbin/rabbitmqctl eval 'ssl:cipher_suites()'`.

В показанном ниже примере возвращены только поддерживаемые шифры. Сервер RabbitMQ не использует и не объявляет эти шифры, если в файле `rabbitmq.config` нет соответствующих настроек.

```
["ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-GCM-SHA384",
 "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA384",
 "ECDH-ECDSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-GCM-SHA384",
 "ECDH-ECDSA-AES256-SHA384", "ECDH-RSA-AES256-SHA384",
 "DHE-RSA-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384",
 "DHE-RSA-AES256-SHA256", "DHE-DSS-AES256-SHA256", "AES256-GCM-SHA384",
 "AES256-SHA256", "ECDHE-ECDSA-AES128-GCM-SHA256",
 "ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES128-SHA256",
 "ECDHE-RSA-AES128-SHA256", "ECDH-ECDSA-AES128-GCM-SHA256",
```

```
"ECDH-RSA-AES128-GCM-SHA256", "ECDH-ECDSA-AES128-SHA256",
"ECDH-RSA-AES128-SHA256", "DHE-RSA-AES128-GCM-SHA256",
"DHE-DSS-AES128-GCM-SHA256", "DHE-RSA-AES128-SHA256", "DHE-DSS-AES128-SHA256",
"AES128-GCM-SHA256", "AES128-SHA256", "ECDHE-ECDSA-AES256-SHA",
"ECDHE-RSA-AES256-SHA", "DHE-RSA-AES256-SHA", "DHE-DSS-AES256-SHA",
"ECDH-ECDSA-AES256-SHA", "ECDH-RSA-AES256-SHA", "AES256-SHA",
"ECDHE-ECDSA-DES-CBC3-SHA", "ECDHE-RSA-DES-CBC3-SHA", "EDH-RSA-DES-CBC3-SHA",
"EDH-DSS-DES-CBC3-SHA", "ECDH-ECDSA-DES-CBC3-SHA", "ECDH-RSA-DES-CBC3-SHA",
"DES-CBC3-SHA", "ECDHE-ECDSA-AES128-SHA", "ECDHE-RSA-AES128-SHA",
"DHE-RSA-AES128-SHA", "DHE-DSS-AES128-SHA", "ECDH-ECDSA-AES128-SHA",
"ECDH-RSA-AES128-SHA", "AES128-SHA"]
```

2. Выберите из поддерживаемых шифров те, которые отвечают требованиям к безопасности вашей организации.

Например, чтобы разрешить только ECDHE-ECDSA-AES128-GCM-SHA256 & ECDHE-ECDSA-AES256-GCM-SHA384, проверьте файл `/etc/rabbitmq/rabbitmq.config` и добавьте в разделе `ssl` и `ssl_options` следующую строку:

```
{ciphers, ["ECDHE-ECDSA-AES128-GCM-SHA256", "ECDHE-ECDSA-AES256-GCM-SHA384"]}
```

3. Перезапустите сервер RabbitMQ с помощью следующей команды:

```
service rabbitmq-server restart
```

Проверка безопасности неактивных данных

Проверьте безопасность пользователей базы данных и учетных данных, используемых с vRealize Automation.

Пользователь Postgres

Учетная запись пользователя Postgres Linux привязана к роли учетной записи суперпользователя базы данных Postgres, по умолчанию это заблокированная учетная запись. Это самая безопасная конфигурация для данного пользователя, так как доступ к ней можно получить только из учетной записи пользователя `root`. Не снимайте блокировку этой учетной записи пользователя.

Роли учетной записи пользователя базы данных

Роли учетной записи пользователя Postgres по умолчанию не должны использоваться за пределами функциональных возможностей приложения. В целях поддержки действий обзора и отчетности базы данных, не используемой по умолчанию, необходимо создать дополнительную учетную запись, а пароль — защищен надлежащим образом.

Запустите следующий сценарий в командной строке:

```
vsac-vami add-db-user newUsername newPassword
```

Будет создан новый пользователь, и этот пользователь задаст пароль.

Примечание Этот сценарий необходимо использовать для базы данных Postgres в тех случаях, когда используется настройка Postgres «главный-подчиненный» высокой доступности.

Настройка проверки подлинности клиента PostgreSQL

Убедитесь, что проверка подлинности локального доверия не настроена для базы данных PostgreSQL устройства vRealize Automation. Эта конфигурация позволяет любому локальному пользователю, включая суперпользователя базы данных, подключаться как любому пользователю PostgreSQL без пароля.

Примечание Учетная запись суперпользователя Postgres должна оставаться как локальное доверие.

Рекомендуется метод проверки подлинности md5, поскольку он отправляет зашифрованные пароли.

Параметры конфигурации проверки подлинности клиента находятся в файле `/storage/db/pgdata/pg_hba.conf`.

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		postgres		trust
# IPv4 local connections:					
#host	all		all	127.0.0.1/32	md5
hostssl	all		all	127.0.0.1/32	md5
# IPv6 local connections:					
#host	all		all	:::1/128	md5
hostssl	all		all	:::1/128	md5
# Allow remote connections for VCAC user.					
#host	vcac		vcac	0.0.0.0/0	md5
hostssl	vcac		vcac	0.0.0.0/0	md5
hostssl	vcac		vcac	:::0/0	md5
# Allow remote connections for VCAC replication user.					
#host	vcac		vcac_replication	0.0.0.0/0	md5
hostssl	vcac		vcac_replication	0.0.0.0/0	md5
hostssl	vcac		vcac_replication	:::0/0	md5
# Allow replication connections by a user with the replication privilege.					
#host	replication		vcac_replication	0.0.0.0/0	md5
hostssl	replication		vcac_replication	0.0.0.0/0	md5
hostssl	replication		vcac_replication	:::0/0	md5

При изменении файла `pg_hba.conf` необходимо перезапустить сервер Postgres, выполнив следующие команды до того, как изменения вступят в силу.

```
# cd /opt/vmware/vpostgres/9.2/bin
# su postgres
# ./pg_ctl restart -D /storage/db/pgdata/ -m fast
```

Настройка ресурсов приложения vRealize Automation

Просмотрите ресурсы приложения vRealize Automation и ограничьте разрешения для файлов.

Процедура

1. Выполните следующую команду, чтобы убедиться, что файлы с наборами битов SUID и GUID верно определены.

```
find / -path /proc -prune -o -type f -perm +6000 -ls
```

Должен появиться следующий список.

```
2197357  24 -rwsr-xr-x  1 polkituser root      23176 Mar 31  2015 /usr/lib/PolicyKit/polkit-
set-default-helper
2197354  16 -rwxr-sr-x  1 root      polkituser  14856 Mar 31  2015 /usr/lib/PolicyKit/polkit-
read-auth-helper
2197353  12 -rwsr-x---  1 root      polkituser  10744 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper-pam
2197352  20 -rwxr-sr-x  1 root      polkituser  19208 Mar 31  2015 /usr/lib/PolicyKit/polkit-
grant-helper
2197351  20 -rwxr-sr-x  1 root      polkituser  19008 Mar 31  2015 /usr/lib/PolicyKit/polkit-
explicit-grant-helper
2197356  24 -rwxr-sr-x  1 root      polkituser  23160 Mar 31  2015 /usr/lib/PolicyKit/polkit-
revoke-helper
2188203  460 -rws--x--x  1 root      root      465364 Apr 21 22:38 /usr/lib64/ssh/ssh-keysign
2138858  12 -rwxr-sr-x  1 root      tty       10680 May 10  2010 /usr/sbin/utempter
2142482  144 -rwsr-xr-x  1 root      root     142890 Sep 15  2015 /usr/bin/passwd
2142477  164 -rwsr-xr-x  1 root      shadow   161782 Sep 15  2015 /usr/bin/chage
2142467  156 -rwsr-xr-x  1 root      shadow   152850 Sep 15  2015 /usr/bin/chfn
1458298  364 -rwsr-xr-x  1 root      root     365787 Jul 22  2015 /usr/bin/sudo
2142481  64 -rwsr-xr-x  1 root      root     57776 Sep 15  2015 /usr/bin/newgrp
1458249  40 -rwsr-x---  1 root      trusted  40432 Mar 18  2015 /usr/bin/crontab
2142478  148 -rwsr-xr-x  1 root      shadow   146459 Sep 15  2015 /usr/bin/chsh
2142480  156 -rwsr-xr-x  1 root      shadow   152387 Sep 15  2015 /usr/bin/gpasswd
2142479  48 -rwsr-xr-x  1 root      shadow   46967 Sep 15  2015 /usr/bin/expiry
311484  48 -rwsr-x---  1 root      messagebus 47912 Sep 16  2014 /lib64/dbus-1/dbus-daemon-
launch-helper
876574  36 -rwsr-xr-x  1 root      shadow   35688 Apr 10  2014 /sbin/unix_chkpwd
876648  12 -rwsr-xr-x  1 root      shadow   10736 Dec 16  2011 /sbin/unix2_chkpwd
 49308  68 -rwsr-xr-x  1 root      root     63376 May 27  2015 /opt/likewise/bin/ksu
1130552  40 -rwsr-xr-x  1 root      root     40016 Apr 16  2015 /bin/su
1130511  40 -rwsr-xr-x  1 root      root     40048 Apr 15  2011 /bin/ping
1130600  100 -rwsr-xr-x  1 root      root     94808 Mar 11  2015 /bin/mount
1130601  72 -rwsr-xr-x  1 root      root     69240 Mar 11  2015 /bin/umount
1130512  36 -rwsr-xr-x  1 root      root     35792 Apr 15  2011 /bin/ping6  2012 /lib64/
dbus-1/dbus-daemon-launch-helper
```

2. Выполните следующую команду, чтобы убедиться, что все файлы на виртуальном устройстве имеют владельца.

```
find / -path /proc -prune -o -nouser -o -nogroup
```

3. Проверьте разрешения для всех файлов для виртуального устройства, чтобы убедиться, что ни в один из них нельзя записать данные с помощью запуска следующей команды.

```
find / -name ".*" -type f -perm -a+w | xargs ls -ldb
```

4. Выполните следующую команду, чтобы убедиться, что правильными файлами владеет только пользователь **vcac**.

```
find / -name "proc" -prune -o -user vcac -print | egrep -v -e "*/vcac/*" | egrep -v -e "*/vmware-vcac/*"
```

Если не появится ни одного результата, владельцем всех правильных файлов является только пользователь **vcac**.

5. Убедитесь, что следующие файлы доступны для записи только пользователю **vcac**.

```
/etc/vcac/vcac/security.properties
/etc/vcac/vcac/solution-users.properties
/etc/vcac/vcac/sso-admin.properties
/etc/vcac/vcac/vcac.keystore
/etc/vcac/vcac/vcac.properties
```

Также проверьте следующие файлы и их вложенные каталоги

```
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

6. Убедитесь, что правильные файлы в следующих каталогах и их вложенных каталогах может читать только пользователь **root** или **vcac**.

```
/etc/vcac/*
/var/log/vcac/*
/var/lib/vcac/*
/var/cache/vcac/*
```

7. Убедитесь, что владельцем правильных файлов является только пользователь **root** или **vco**, как показано в следующих каталогах и их вложенных каталогах.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
/var/cache/vco/*
```

8. Убедитесь, что доступ к записи правильных файлов имеет только пользователь **root** или **vco**, как показано в следующих каталогах и их вложенных каталогах.

```
/etc/vco/*
/var/log/vco/*
/var/lib/vco/*
```

```
/var/cache/vco/*
```

9. Убедитесь, что доступ к чтению правильных файлов имеет только пользователь `root` или `vco`, как показано в следующих каталогах и их вложенных каталогах.

```
/etc/vco/*
```

```
/var/log/vco/*
```

```
/var/lib/vco/*
```

```
/var/cache/vco/*
```

Настройка конфигурации прокси-сервера консоли

Можно настроить конфигурацию удаленной консоли vRealize Automation для более быстрого устранения неполадок и решения организационных вопросов.

Во время установки, настройки или обслуживания vRealize Automation вы можете изменять определенные параметры, чтобы активировать устранение неполадок и отладку в системе. Вносите в каталог и подвергайте проверке каждое такое изменение, чтобы обеспечить надлежащую защиту соответствующих компонентов в соответствии с их применением. Не переходите к этапу производства, если не уверены в безопасности изменений конфигурации.

Настройка срока действия билета VMware Remote Console

Можно настроить период действия билетов удаленной консоли, которые используются при установке соединений VMware Remote Console.

Когда пользователь устанавливает соединения VMware Remote Console, система создает и возвращает одноразовые учетные данные, с помощью которых устанавливается отдельное соединение с виртуальной машиной. Можно задать в качестве срока действия билета конкретный период времени в минутах.

Процедура

1. Откройте в текстовом редакторе файл `/etc/vcac/security.properties`.
2. Добавьте в файл строку в таком формате: `consoleproxy.ticket.validitySec=30`

В этой строке числовое значение указывает на количество минут, после которых билет перестанет действовать.

3. Сохраните файл и закройте его.
4. Перезапустите `vcac`-сервер с помощью команды `/etc/init.d/vcac-server restart`

В качестве срока действия билета будет указан заданный период времени в минутах.

Настройка порта прокси-сервера консоли

Можно настроить порт, на котором прокси-сервер консоли VMware Remote Console будет прослушивать сообщения.

Процедура

1. Откройте в текстовом редакторе файл `/etc/vcac/security.properties`.
2. Добавьте в файл строку в таком формате: `consoleproxy.service.port=8445`

Числовое значение указывает на номер порта службы прокси-сервера консоли, в данном случае — 8445.

3. Сохраните файл и закройте его.
4. Перезапустите `vcac`-сервер с помощью команды `/etc/init.d/vcac-server restart`.

Номер порта службы прокси-сервера будет изменен на заданный номер.

Настройка заголовка ответа **X-XSS-Protection**

Добавьте заголовок ответа `X-XSS-Protection` в файл конфигурации `HAProxy`.

Процедура

1. Откройте для редактирования файл `/etc/haproxy/conf.d/20-vcac.cfg`.
2. Добавьте следующие строки в клиентской части:

```
rspdel X-XSS-Protection:\ 1;\ mode=block
rspadd X-XSS-Protection:\ 1;\ mode=block
```

3. Перезагрузите конфигурацию `HAProxy` с помощью следующей команды:
`/etc/init.d/haproxy reload`

Настройка заголовка ответа **X-Content-Type-Options**

Добавьте заголовок ответа `X-Content-Type-Options` в конфигурацию `HAProxy`.

Процедура

1. Откройте для редактирования файл `/etc/haproxy/conf.d/20-vcac.cfg`.
2. Добавьте следующие строки в клиентской части:

```
http-response set-header X-Content-Type-Options nosniff
```

3. Перезагрузите конфигурацию `HAProxy` с помощью следующей команды:
`/etc/init.d/haproxy reload`

Настройка заголовка ответа **HTTP Strict Transport Security**

Добавьте в конфигурацию `HAProxy` заголовок ответа `HTTP Strict Transport (HSTS)`.

Процедура

1. Откройте для редактирования файл `/etc/haproxy/conf.d/20-vcac.cfg`.

2. Добавьте следующие строки в клиентской части:

```
rspdel Strict-Transport-Security:\ max-age=31536000
rspadd Strict-Transport-Security:\ max-age=31536000
```

3. Перезагрузите конфигурацию HAProxy с помощью следующей команды:

```
/etc/init.d/haproxy reload
```

Настройка заголовка ответа X-Frame-Options

В некоторых случаях заголовок ответа X-Frame-Options может появляться дважды.

Заголовок ответов X-Frame-Options появляется дважды из-за того, что служба vIDM добавляет этот заголовок в серверной части и в HAProxy. Такого удвоения можно избежать с помощью правильных настроек.

Процедура

1. Откройте для редактирования файл `/etc/haproxy/conf.d/20-vcac.cfg`.
2. Найдите следующую строку в клиентской части:


```
rspadd X-Frame-Options:\ SAMEORIGIN
```
3. Перед строкой, которую вы нашли в предыдущем шаге, добавьте такие строки:


```
rspdel X-Frame-Options:\ SAMEORIGIN
```
4. Перезагрузите конфигурацию HAProxy с помощью следующей команды:


```
/etc/init.d/haproxy reload
```

Настройка заголовков ответов сервера

Рекомендуется настроить систему vRealize Automation, чтобы она ограничивала информацию, доступную потенциальным злоумышленникам.

В максимально возможной степени минимизируйте количество информации об удостоверениях и версии, доступ к которой предоставляет используемая система. Хакеры и злоумышленники могут использовать эти сведения для подготовки атак, направленных на веб-сервер или версию.

Настройка заголовка ответа сервера Lighttpd

Рекомендуется создать пустой заголовок для сервера Lighttpd устройства vRealize Automation.

Процедура

1. Откройте в текстовом редакторе файл `/opt/vmware/etc/lighttpd/lighttpd.conf`.
2. Добавьте в файл запись `server.tag = " "`.
3. Сохраните изменения и закройте файл.

4. Перезапустите сервер Lighttpd с помощью команды `# /opt/vmware/etc/init.d/vami-lighttpd restart`.

Настройка заголовка ответа TCServer для устройства vRealize Automation

Рекомендуется создать пользовательский пустой заголовок ответа сервера TCServer, используемый с устройством vRealize Automation, чтобы ограничить риск получения злоумышленниками ценной информации.

Процедура

1. Откройте в текстовом редакторе файл `/etc/vco/app-server/server.xml`.
2. Добавьте `server=" "` в каждый элемент `<Connector>`.
Например, `<Connector protocol="HTTP/1.1" server="" />`.
3. Сохраните изменения и закройте файл.
4. Перезапустите сервер с помощью следующей команды:

```
service vco-server restart
```

Настройка заголовка ответа сервера служб IIS

В целях безопасности рекомендуется создать пользовательский пустой заголовок для сервера служб IIS, используемого с Identity Appliance, чтобы ограничить риск получения злоумышленниками ценной информации.

Процедура

1. Откройте в текстовом редакторе файл `C:\Windows\System32\inetsrv\urlscan\UrlScan.ini`.
2. Найдите запись `RemoveServerHeader=0` и измените ее на `RemoveServerHeader=1..`
3. Сохраните изменения и закройте файл.
4. Перезапустите сервер с помощью команды `iisreset`.

Следующие шаги

Отключите заголовок служб IIS X-Powered By, удалив заголовки ответа HTTP из списка на консоли диспетчера служб IIS.

1. Откройте консоль диспетчера служб IIS.
2. Откройте заголовок ответа HTTP и удалите его из списка.
3. Перезапустите сервер с помощью команды `iisreset`.

Настройка времени ожидания сеанса Устройство vRealize Automation

Настройте параметр времени ожидания сеанса на Устройство vRealize Automation в соответствии с политикой безопасности организации.

Время ожидания сеанса Устройство vRealize Automation по умолчанию в отсутствие активности пользователя составляет 30 минут. Чтобы привести это значение времени ожидания в соответствие политике безопасности организации, измените файл `web.xml` на компьютере узла Устройство vRealize Automation.

Процедура

1. Откройте файл `/usr/lib/vcac/server/webapps/vcac/WEB-INF/web.xml` в текстовом редакторе.
2. Найдите `session-config` и настройте значение `session-timeout`. См. следующий образец кода.

```
<!-- 30 minutes session expiration time -->
<session-config>
  <session-timeout>30</session-timeout>
  <tracking-mode>COOKIE</tracking-mode>
  <cookie-config>
    <path>/</path>
  </cookie-config>
</session-config>
```

3. Перезапустите сервер с помощью следующей команды.

```
service vcac-server restart
```

Управление вспомогательным программным обеспечением

Для минимизации рисков безопасности удалите или настройте вспомогательное программное обеспечение на компьютерах узлов vRealize Automation.

Настройте все программное обеспечение, которое не будет удалено, в соответствии с рекомендациями и практическими указаниями по безопасности, предоставляемыми поставщиком этого программного обеспечения, чтобы минимизировать способность такого ПО создавать нарушения безопасности.

Защита обработчика запоминающих USB-устройств

Защитите обработчик запоминающих USB-устройств, чтобы предотвратить его использование как обработчика USB-устройств с компьютерами узлов виртуального устройства VMware. Потенциальные злоумышленники могут использовать этот обработчик, чтобы скомпрометировать систему.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть строка `install usb-storage /bin/true`.
3. Сохраните файл и закройте его.

Защита обработчика протоколов Bluetooth

Защитите обработчик протоколов Bluetooth на компьютерах узлов виртуального устройства, чтобы предотвратить его использование потенциальными злоумышленниками.

Привязывание протокола **Bluetooth** к стеку сети не является необходимым. Это действие может увеличить поверхность атаки узла.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть следующая строка.

```
install bluetooth /bin/true
```
3. Сохраните файл и закройте его.

Защита протокола **SCTP (Stream Control Transmission)**

Сделайте так, чтобы протокол **SCTP (Stream Control Transmission)** не загружался в системе по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Настройте систему на предотвращение загрузки модуля протокола **SCTP (Stream Control Transmission)**, за исключением случаев, когда это абсолютно необходимо. Протокол **SCTP** является неиспользуемым протоколом транспортного уровня стандарта **IETF**. Привязывание этого протокола к стеку сети увеличивает поверхность атаки узла. Непривилегированные локальные процессы могут заставить ядро динамически загрузить обработчик протоколов, открыв сокет с помощью этого протокола.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть следующая строка.

```
install sctp /bin/true
```
3. Сохраните файл и закройте его.

Защита протокола **DCCP (Datagram Congestion Protocol)**

В рамках действий по усилению защиты системы сделайте так, чтобы протокол **DCCP (Datagram Congestion Protocol)** не загружался на компьютерах узлов виртуального устройства по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Не загружайте модуль протокола **DCCP (Datagram Congestion Protocol)**, если это не является абсолютно необходимым. Протокол **DCCP** является предлагаемым протоколом транспортного уровня, который не используется. Привязывание этого протокола к стеку сети увеличивает поверхность атаки узла.

Непривилегированные локальные процессы могут заставить ядро динамически загрузить обработчик протоколов, используя этот протокол для открытия сокета.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.

2. Убедитесь, что в файле есть строки протокола DCCP.

```
install dccp/bin/true
install dccp_ipv4/bin/true
install dccp_ipv6/bin/true
```

3. Сохраните файл и закройте его.

Защита сетевого моста

Сделайте так, чтобы модуль сетевого моста не загружался в системе по умолчанию. Потенциальные злоумышленники могут использовать его, чтобы скомпрометировать систему.

Настройте систему таким образом, чтобы она не давала сети загружаться, кроме случаев, когда это абсолютно необходимо. Потенциальные злоумышленники могут использовать это, чтобы обойти секционирование и защиту сети.

Процедура

1. Выполните следующую команду на всех компьютерах узлов виртуального устройства VMware.

```
# rmmod bridge
```

2. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.

3. Убедитесь, что в файле есть следующая строка.

```
install bridge /bin/false
```

4. Сохраните файл и закройте его.

Защита протокола RDS (Reliable Datagram Sockets)

В рамках действий по усилению защиты системы сделайте так, чтобы протокол RDS (Reliable Datagram Sockets) не загружался на компьютерах узлов виртуального устройства по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Привязывание протокола RDS (Reliable Datagram Sockets) к стеку сети увеличивает поверхность атаки узла. Непривилегированные локальные процессы могут заставить систему динамически загрузить обработчик протоколов, используя протокол для открытия сокета.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.

2. Убедитесь, что в файле есть строка `install rds /bin/true`.

3. Сохраните файл и закройте его.

Защита протокола TIPC (Transparent Inter-Process Communication)

В рамках действий по защите системы сделайте так, чтобы протокол TIPC (Transparent Inter-Process Communication) не загружался на компьютерах узлов виртуального устройства по умолчанию.

Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Привязывание протокола TIPC (Transparent Inter-Process Communication) к стеку сети увеличивает поверхность атаки узла. Непривилегированные локальные процессы могут заставить ядро динамически загрузить обработчик протоколов, используя этот протокол для открытия сокета.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть строка `install tipc /bin/true`.
3. Сохраните файл и закройте его.

Защита протокола IPX (Internetwork Packet Exchange)

Сделайте так, чтобы протокол IPX (Internetwork Packet Exchange) не загружался в системе по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Не загружайте модуль протокола IPX (Internetwork Packet Exchange), если это не является абсолютно необходимым. Протокол IPX является устаревшим протоколом сетевого уровня. Привязывание этого протокола к стеку сети увеличивает поверхность атаки узла. Непривилегированные локальные процессы могут заставить систему динамически загрузить обработчик протоколов, используя этот протокол для открытия сокета.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть следующая строка.

```
install ipx /bin/true
```
3. Сохраните файл и закройте его.

Защита протокола Appletalk

Сделайте так, чтобы протокол Appletalk не загружался в системе по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Не загружайте модуль протокола Appletalk, если это не является абсолютно необходимым. Привязывание этого протокола к стеку сети увеличивает поверхность атаки узла. Непривилегированные локальные процессы могут заставить систему динамически загрузить обработчик протоколов, используя этот протокол для открытия сокета.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть следующая строка.

```
install appletalk /bin/true
```
3. Сохраните файл и закройте его.

Защита протокола DECnet

Сделайте так, чтобы протокол DECnet не загружался в системе по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Не загружайте модуль протокола DECnet, если это не является абсолютно необходимым. Привязывание этого протокола к стеку сети увеличивает поверхность атаки узла. Непривилегированные локальные процессы могут заставить систему динамически загрузить обработчик протоколов, используя этот протокол для открытия сокета.

Процедура

1. Откройте файл протокола DECnet `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть следующая строка.

```
install decnet /bin/true
```
3. Сохраните файл и закройте его.

Защита модуля Firewire

Сделайте так, чтобы модуль Firewire не загружался в системе по умолчанию. Потенциальные злоумышленники могут использовать этот протокол, чтобы скомпрометировать систему.

Не загружайте модуль Firewire, если это не является абсолютно необходимым.

Процедура

1. Откройте файл `/etc/modprobe.conf.local` в текстовом редакторе.
2. Убедитесь, что в файле есть следующая строка.

```
install ieee1394 /bin/true
```
3. Сохраните файл и закройте его.

Защита компонента инфраструктуры как услуги

При усилении защиты системы защитите компонент инфраструктуры как услуги vRealize Automation и его компьютер узла, чтобы предотвратить их использование потенциальными злоумышленниками.

Необходимо настроить параметр безопасности для компонента инфраструктуры как услуги vRealize Automation и узел, на котором он размещен. Необходимо задать или проверить конфигурацию других связанных компонентов и приложений. В некоторых случаях можно проверить существующие параметры, в других необходимо изменить или добавить параметры для правильной настройки.

Настройка протокола NTP

В целях безопасности рекомендуется использовать в производственной среде vRealize Automation авторизованные серверы времени, а не синхронизацию времени на узле.

В производственной среде следует отключить синхронизацию времени на узле и использовать авторизованные серверы времени. Это обеспечит точное отслеживание действий пользователей и поможет посредством аудита и журналов выявлять потенциальные злонамеренные действия и вторжения.

Настройка TLS для передачи данных инфраструктуры как услуги

В развертывании vRealize Automation должны использоваться надежные протоколы TLS в целях защиты каналов передачи для компонентов инфраструктуры как услуги.

Криптографические протоколы SSL (Secure Sockets Layer — уровень защищенных сокетов) и — более новый — TLS (Transport Layer Security — безопасность транспортного уровня) позволяют обеспечить безопасность системы во время сетевого обмена данными между различными ее компонентами. Протокол SSL — более старый, во многих случаях он уже не обеспечивает надлежащую защиту от потенциальных угроз. В протоколах SSL более ранних версий, включая SSLv2 и SSLv3, обнаружены существенные слабые места. Эти версии больше не считаются надежными.

В зависимости от политик безопасности организации можно также отключить протокол TLS 1.0.

Примечание При отключении TLS в подсистеме балансировки нагрузки также следует отключить ненадежные протоколы, например SSLv2, SSLv3 и при необходимости TLS 1.0 и 1.1.

Включение протоколов TLS 1.1 и 1.2 для инфраструктуры как услуги

Включите протоколы TLS 1.1 и 1.2 и задайте принудительное их использование на всех виртуальных машинах, на которых размещены компоненты инфраструктуры как услуги.

Процедура

1. Щелкните **Начало**, затем щелкните **Запустить**.
2. Введите **Regedit** и нажмите кнопку **ОК**.
3. Найдите и откройте следующий подраздел реестра.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols
4. Проверьте следующую информацию и при необходимости создайте новые записи.
 - Если в разделе **Protocols** нет подраздела с именем **TLS 1.1**, создайте его.
 - Если в подразделе **TLS 1.1** нет подраздела с именем **Client**, создайте его.
 - Если в подразделе **Client** нет ключа с именем **DisabledByDefault**, создайте такой ключ (он должен иметь тип **DWORD**).
 - Щелкните правой кнопкой мыши ключ **DisabledByDefault**, выберите «Изменить» и задайте для этого ключа значение **0**.
 - Если в подразделе **Client** нет ключа с именем **Enabled**, создайте такой ключ (он должен иметь тип **DWORD**).
 - Щелкните правой кнопкой мыши ключ **Enabled**, выберите «Изменить» и задайте для этого ключа значение **1**.

- Если в подразделе TLS 1.1 нет подраздела с именем **Server**, создайте его.
 - Если в подразделе **Server** нет ключа с именем **DisabledByDefault**, создайте такой ключ (он должен иметь тип **DWORD**).
 - Щелкните правой кнопкой мыши ключ **DisabledByDefault**, выберите «Изменить» и задайте для этого ключа значение **0**.
 - Если в подразделе **Server** нет ключа с именем **Enabled**, создайте такой ключ (он должен иметь тип **DWORD**).
 - Щелкните правой кнопкой мыши ключ **Enabled**, выберите «Изменить» и задайте для этого ключа значение **1**.
5. Повторите описанные выше шаги для протокола TLS 1.2.

Примечание Чтобы включить принудительное использование TLS 1.1 и 1.2, необходимо настроить дополнительные параметры, как описано далее.

6. Найдите и откройте следующий подраздел реестра.
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319
7. Проверьте следующую информацию и при необходимости создайте новые записи.
- Если отсутствует ключ типа **DWORD** с именем **SchUseStrongCrypto**, создайте такой ключ и задайте для него значение **1**.
 - Если отсутствует ключ типа **DWORD** с именем **SystemDefaultTlsVersions**, создайте такой ключ и задайте для него значение **1**.
8. Найдите и откройте следующий подраздел реестра.
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319
9. Проверьте следующую информацию и при необходимости создайте новые записи.
- Если отсутствует ключ типа **DWORD** с именем **SchUseStrongCrypto**, создайте такой ключ и задайте для него значение **1**.
 - Если отсутствует ключ типа **DWORD** с именем **SystemDefaultTlsVersions**, создайте такой ключ и задайте для него значение **1**.

Отключение SSL 3.0 и TLS 1.0 для инфраструктуры как услуги

Отключите SSL 3.0 и устаревший протокол TLS 1.0 для компонентов инфраструктуры как услуги.

Процедура

1. Щелкните **Начало**, затем щелкните **Запустить**.
 2. Введите **Regedit** и нажмите кнопку **ОК**.
 3. Найдите и откройте следующий подраздел реестра.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols

4. Проверьте следующую информацию и при необходимости создайте новые записи.

- Если в разделе **Protocols** нет подраздела с именем **SSL 3.0**, создайте его.
- Если в подразделе **SSL 3.0** нет подраздела с именем **Client**, создайте его.
- Если в подразделе **Client** нет ключа с именем **DisabledByDefault**, создайте такой ключ (он должен иметь тип **DWORD**).
- Щелкните правой кнопкой мыши ключ **DisabledByDefault**, выберите «Изменить» и задайте для этого ключа значение **1**.
- Щелкните правой кнопкой мыши ключ **Enabled**, выберите «Изменить» и задайте для этого ключа значение **0**.
- Если в подразделе **SSL 3.0** нет подраздела с именем **Server**, создайте его.
- Если в подразделе **Server** нет ключа с именем **DisabledByDefault**, создайте такой ключ (он должен иметь тип **DWORD**).
- Щелкните правой кнопкой мыши ключ **DisabledByDefault**, выберите «Изменить» и задайте для этого ключа значение **1**.
- Если в подразделе **Server** нет ключа с именем **Enabled**, создайте такой ключ (он должен иметь тип **DWORD**).
- Щелкните правой кнопкой мыши ключ **Enabled**, выберите «Изменить» и задайте для этого ключа значение **0**.

5. Повторите описанные выше шаги для протокола TLS 1.0.

Отключение протокола TLS 1.0 для инфраструктуры как услуги

Чтобы обеспечить максимальный уровень безопасности, настройте для инфраструктуры как услуги создание пулов и отключите протокол TLS 1.0.

Дополнительные сведения см. в статье базы знаний Майкрософт по адресу <https://support.microsoft.com/en-us/kb/245030>.

Процедура

1. Настройте для инфраструктуры как услуги создание пулов вместо использования веб-сокетов.

- а) В файле конфигурации служб диспетчера `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config` добавьте следующие значения в раздел `<appSettings>`:

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

- б) Перезапустите службу диспетчера (служба VMware vCloud Automation Center).

2. Убедитесь, что протокол TLS 1.0 отключен на сервере инфраструктуры как услуги.

- а) Запустите редактор реестра от имени администратора.
- б) В окне реестра откройте раздел `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\`.
- в) Правой кнопкой мыши щелкните элемент «Протоколы», выберите **Создать > Раздел** и введите **TLS 1.0**.
- г) В дереве навигации щелкните правой кнопкой мыши только что созданный раздел TLS 1.0, затем в раскрывающемся меню выберите **Создать > Раздел** и введите **Client**.
- д) В дереве навигации щелкните правой кнопкой мыши только что созданный раздел TLS 1.0, затем в раскрывающемся меню выберите **Создать > Раздел** и введите **Server**.
- е) В дереве навигации в разделе TLS 1.0 щелкните правой кнопкой мыши элемент **Client**, затем выберите **Создать > Значение DWORD (32-разрядное)** и введите **DisabledByDefault**.
- ж) В дереве навигации в разделе TLS 1.0 выберите элемент **Client**, затем в правой области дважды щелкните **DWORD DisabledByDefault** и введите **1**.
- з) В дереве навигации в разделе TLS 1.0 щелкните правой кнопкой мыши элемент **Server**, затем выберите **Создать > Значение DWORD (32-разрядное)** и введите **Enabled**.
- и) В дереве навигации в разделе TLS 1.0 выберите элемент **Server**, затем в правой области дважды щелкните **включенный** параметр **DWORD** и введите **0**.
- к) Перезапустите Windows Server.

Настройка наборов шифров TLS

Чтобы обеспечить максимальную безопасность, необходимо настроить для компонентов vRealize Automation использование криптостойких шифров. Шифр, согласованный между сервером и браузером, определяет надежность шифрования для TLS-сеанса. Чтобы всегда использовались только криптостойкие шифры, отключите легко раскрываемые шифры в компонентах vRealize Automation. Настройте для сервера поддержку только криптостойких шифров и использование ключей достаточно большого размера. Также следует настроить надлежащий порядок для всех шифров.

Недопустимые наборы шифров

Отключите наборы шифров, которые не обеспечивают проверку подлинности, например наборы шифров NULL, aNULL, eNULL. Также отключите анонимный обмен ключами по протоколу Диффи-Хеллмана (ADH), шифры экспортного уровня (EXP, шифры, содержащие DES), ключи размером менее 128 бит для шифрования полезной нагрузки, использование MD5 в качестве механизма хэширования для полезной нагрузки, наборы шифров IDEA и RC4. Убедитесь также, что выключены наборы шифров, для которых используется обмен ключами по протоколу Диффи-Хеллмана (DHE).

Сведения о том, как отключить статические шифры ключей в vRealize Automation, см. в [статье базы знаний 71094](#).

Проверка безопасности сервера узла

В целях обеспечения безопасности рекомендуется проверить конфигурацию системы безопасности серверов узла инфраструктуры как услуги (IaaS).

Корпорация Майкрософт предлагает несколько инструментов, которые помогут вам убедиться в безопасности серверов узла. Обратитесь к поставщику корпорации Майкрософт, чтобы получить инструкции относительно наиболее подходящего использования этих инструментов.

Проверка базового плана безопасности сервера узла

Запустите Microsoft Baseline Security Analyzer (MBSA), чтобы быстро подтвердить, что на сервере установлены последние обновления и исправления. MBSA можно использовать для установки отсутствующих исправлений для системы безопасности от корпорации Майкрософт, чтобы обеспечить соответствие рекомендациям Майкрософт по безопасности.

Загрузите последнюю версию инструмента MBSA с веб-сайта корпорации Майкрософт.

Проверка конфигурации безопасности сервера узла

Воспользуйтесь мастером настройки безопасности Windows (SCW) и диспетчером совместимости системы безопасности Microsoft (SCM), чтобы проверить надежность конфигурации сервера узла.

Запустите SCW из списка средств администрирования с сервера Windows. Этот инструмент может определить роли сервера и установленные функции, включая сеть, брандмауэры Windows и параметры реестра. Сравните отчет с последними инструкциями по аппаратной защите от соответствующего SCM для вашего сервера Windows. На основании результатов вы сможете точно настроить параметры безопасности для каждой функции, например сетевых служб, параметров учетной записи и брандмауэров Windows, и применить параметры к серверу.

Более подробную информацию об инструменте SCW можно найти на веб-сайте Microsoft TechNet.

Защита ресурсов приложения

Рекомендуется убедиться, что все относящиеся к делу файлы инфраструктуры как услуги имеют соответствующие разрешения.

Сверьте файлы инфраструктуры как услуги со своей установкой инфраструктуры как услуги. В большинстве случаев вложенные папки и файлы для каждой папки должны иметь те же настройки, что и сама папка.

Каталог или файл	Группа или пользователь	Полное управление	Изменения	Чтение и выполнение	Чтение	Запись
VMware\vmCAC\Agents \<agent_name>\logs	СИСТЕМА	X	X	X	X	X
	Администратор	X	X	X	X	X
	Администраторы	X	X	X	X	X
VMware\vmCAC\Agents\ <agent_name>\temp	СИСТЕМА	X	X	X	X	X
	Администратор	X	X	X	X	X

Каталог или файл	Группа или пользователи	Полное управление	Изменения	Чтение и выполнение	Чтение	Запись
VMware\vCAC\Agents\	Администраторы	X	X	X	X	X
	СИСТЕМА	X	X	X	X	X
	Администраторы	X	X	X	X	X
	Пользователи			X	X	
VMware\vCAC\Distributed Execution Manager\	СИСТЕМА	X	X	X	X	X
	Администраторы	X	X	X	X	X
	Пользователи			X	X	
VMware\vCAC\Distributed Execution Manager\DEM\Logs	СИСТЕМА	X	X	X	X	X
	Администратор	X	X	X	X	X
	Администраторы	X	X	X	X	X
VMware\vCAC\Distributed Execution Manager\DEO\Logs	СИСТЕМА	X	X	X	X	X
	Администратор	X	X	X	X	X
	Администраторы	X	X	X	X	X
VMware\vCAC\Management Agent\	СИСТЕМА	X	X	X	X	X
	Администраторы	X	X	X	X	X
	Пользователи			X	X	
VMware\vCAC\Server\	СИСТЕМА	X	X	X	X	X
	Администраторы	X	X	X	X	X
	Пользователи			X	X	
VMware\vCAC\Web API	СИСТЕМА	X	X	X	X	X
	Администраторы	X	X	X	X	X
	Пользователи			X	X	

Обеспечение безопасности узла инфраструктуры как услуги

В целях безопасности рекомендуется настроить основные параметры узла инфраструктуры как услуги в соответствии с инструкциями по обеспечению защиты.

Настройте защиту для различных учетных записей, приложений, портов и служб на узле инфраструктуры как услуги.

Проверка настроек учетной записи пользователя сервера

Удалите все лишние локальные и доменные учетные записи пользователя и ненужные настройки таких учетных записей. Из учетных записей пользователя, не связанных с работой приложений, оставьте только те, которые необходимы для администрирования, обслуживания и устранения неполадок. Разрешите доменным учетным записям пользователя минимальный удаленный доступ, необходимый для обслуживания сервера. Постоянно контролируйте и тщательно проверяйте использование этих учетных записей.

Удаление ненужных приложений

Удалите с серверов узлов все ненужные приложения. Они повышают риск угрозы безопасности, так как могут содержать неизвестные или нерешенные проблемы защиты.

Отключение ненужных портов и служб

Проверьте, какие порты открыты в брандмауэре сервера узла. Заблокируйте все порты, которые не требуются для работы компонента инфраструктуры как услуги или критически важных функций системы. См. раздел [Настройка портов и протоколов](#). Проверьте, какие службы работают с сервером узла, и отключите ненужные.

Настройка параметров безопасности сети для узла

8

Чтобы обеспечить максимальную защиту от известных угроз безопасности, настройте сетевой интерфейс и параметры обмена данными на всех узлах VMware.

В рамках комплексной защиты следует настроить параметры безопасности сетевого интерфейса для виртуальных устройств VMware и компонентов инфраструктуры как услуги в соответствии с действующими правилами безопасности.

В эту главу входят следующие разделы:

- [Настройка параметров сети для устройств VMware](#)
- [Настройка параметров сети для узла инфраструктуры как услуги](#)
- [Настройка портов и протоколов](#)

Настройка параметров сети для устройств VMware

Чтобы обеспечить на узлах виртуального устройства VMware обмен только важными данными и только с надлежащей защитой, проверьте и откорректируйте настройки сетевого обмена данными для этих узлов.

Проверьте настройки IP-протокола сети для узлов VMware и настройте параметры сети в соответствии с правилами безопасности. Отключите все протоколы обмена второстепенными данными.

Заккрытие пользователям доступа к управлению сетевыми интерфейсами

Рекомендуется оставить пользователям только те разрешения системы, которые им необходимы, чтобы выполнять рабочие обязанности на компьютерах узлов устройства VMware.

Разрешение учетным записям пользователей с правами управлять сетевыми интерфейсами может привести к обходу механизмов безопасности сети или отказу в обслуживании. Ограничьте возможность изменять параметры сетевого интерфейса для пользователей с правами.

Процедура

1. Выполните следующую команду на каждом компьютере узла устройства VMware.

```
# grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*
```

2. Убедитесь, что каждому интерфейсу присвоено значение NO.

Настройка размера очереди невыполненной работы TCP

Чтобы обеспечить некоторый уровень защиты от атак злоумышленников, настройте размер очереди невыполненной работы TCP по умолчанию на компьютерах узлов устройства VMware.

Задайте размерам очередей невыполненной работы правильное значение размера по умолчанию, чтобы смягчить последствия атак типа «отказ в обслуживании», осуществляемых по TCP. Рекомендованный параметр по умолчанию — 1280.

Процедура

1. Выполните следующую команду на каждом компьютере узла устройства VMware.

```
# cat /proc/sys/net/ipv4/tcp_max_syn_backlog
```

2. Откройте файл `/etc/sysctl.conf` в текстовом редакторе.
3. Задайте размер очереди невыполненной работы TCP по умолчанию, добавив в файл следующую запись.

```
net.ipv4.tcp_max_syn_backlog=1280
```

4. Сохраните изменения и закройте файл.

Отклонение эхо-запросов ICMPv4 для получения широковещательного адреса

В целях безопасности рекомендуется настроить на узлах устройства VMware игнорирование эхо-запросов широковещательного адреса ICMP.

Ответы на эхо-запросы вещания по протоколу межсетевых управляющих сообщений (Internet Control Message Protocol, ICMP) предоставляют вектор для расширения злонамеренных действий и способствует определению топологии сети вредоносными агентами. Настроив на узлах устройства игнорирование эхо-запросов ICMPv4, можно защититься от подобных угроз.

Процедура

1. Выполните команду `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` на узлах виртуального устройства VMware, чтобы проверить отклоняются ли на них эхо-запросы широковещательного адреса IPv4.

Если для узлов настроено отклонение перенаправлений IPv4, команда вернет значение 0 для параметра `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`.

2. Если необходимо настроить на узле виртуального устройства отклонение эхо-запросов широковещательного адреса ICMPv4, откройте файл `/etc/sysctl.conf` в текстовом редакторе на узле Windows.
3. Найдите такую запись: `net.ipv4.icmp_echo_ignore_broadcasts=0`. Если указанной записи нет или для нее не установлено нулевое значение, добавьте эту запись или измените ее значение соответствующим образом.
4. Сохраните изменения и закройте файл.

Отключение техники IPv4 Proxy ARP

Для избежания неразрешенной передачи информации следует отключить технику IPv4 Proxy ARP на узлах устройства VMware, если не предусмотрены иные требования.

Техника IPv4 Proxy ARP позволяет системе отправлять ответы на запросы ARP в одном интерфейсе от имени узлов, подключенных к другому интерфейсу. Если эта техника не нужна, отключите ее, чтобы предотвратить утечку адресной информации при передаче данных между подключенными сегментами сети.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` на узлах виртуального устройства VMware, чтобы проверить, отключена ли на них техника IPv4 Proxy ARP.

Если на узлах отключена техника IPv6 Proxy ARP, команда вернет значение 0.

```
/proc/sys/net/ipv4/conf/all/proxy_arp:0
/proc/sys/net/ipv4/conf/default/proxy_arp:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить технику IPv6 Proxy ARP на узлах, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv4.conf.default.proxy_arp=0
net.ipv4.conf.all.proxy_arp=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните внесенные изменения и закройте файл.

Отклонение сообщений о перенаправлении ICMP IPv4

В целях безопасности рекомендуется настроить на узлах виртуального устройства VMware отклонение сообщений о перенаправлении ICMP IPv4.

С помощью сообщений о перенаправлении ICMP маршрутизаторы сообщают узлам о наличии более краткого маршрута к точке назначения. Злоумышленники могут использовать такие сообщения для атак посредника (атаки «злоумышленник в середине»). Сообщения в таких случаях вносят изменения в таблицу маршрутов узла без какой-либо проверки. Настройте в своей системе игнорирование таких сообщений, если в них нет необходимости.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects | egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них сообщения о перенаправлении IPv4.

Если для узлов настроено отклонение перенаправлений IPv4, результат команды будет таким:

```
/proc/sys/net/ipv4/conf/all/accept_reidrects:0
```

```
/proc/sys/net/ipv4/conf/default/accept_redirects:0
```

2. Если необходимо настроить на узле виртуального устройства отклонение сообщений о перенаправлении IPv4, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте значения строк, которые начинаются с `net.ipv4.conf`

Если указанных далее записей нет или для них не установлены нулевые значения, добавьте эти записи в файл или измените их значения соответствующим образом.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

4. Сохраните внесенные изменения и закройте файл.

Отклонение ICMP-сообщений о перенаправлении IPv6

Рекомендуется убедиться, что компьютеры узлов виртуального устройства VMware отклоняют ICMP-сообщения о перенаправлении IPv6.

С помощью сообщений о перенаправлении ICMP маршрутизаторы сообщают узлам о наличии более короткого маршрута к точке назначения. Злоумышленники могут использовать такие сообщения для атак посредника (атаки «злоумышленник в середине»). Сообщения в таких случаях вносят изменения в таблицу маршрутов узла без какой-либо проверки. Убедитесь, что используемая система настроена игнорировать их, если они не нужны для других целей.

Процедура

1. Запустите команду `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects | egrep "default|all"` на компьютерах узлов виртуального устройства VMware, чтобы убедиться, что они отклоняют сообщения о перенаправлении IPv6

Если компьютеры узлов настроены отклонять перенаправления IPv6, эта команда возвращает следующее сообщение:

```
/proc/sys/net/ipv6/conf/all/accept_redirects:0
```

```
/proc/sys/net/ipv6/conf/default/accept_redirects:0
```

2. Чтобы настроить компьютеры узлов виртуального устройства на отклонение сообщений о перенаправлении IPv4, откройте файл `/etc/sysctl.conf` в текстовом редакторе.

3. Проверьте значения строк, которые начинаются с `net.ipv6.conf`

Если значения для следующих записей в данной области не установлены на ноль или записи не существуют, добавьте их в этот файл или обновите существующие записи надлежащим образом.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

4. Сохраните изменения и закройте файл.

Регистрация пакетов Martian IPv4

Рекомендуется убедиться, что компьютеры узлов виртуального устройства VMware записывают в журнал пакеты Martian IPv4.

Пакеты Martian содержат адреса, которые известны системе как недействительные. Настройте компьютеры узлов на запись этих сообщений, чтобы иметь возможность определять неправильные конфигурации или текущие атаки.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians | egrep "default|all"` на компьютерах узлов устройства VMware, чтобы убедиться, что они записывают в журнал пакеты Martian IPv4.

Если виртуальные машины настроены на запись в журнал пакетов Martian, они возвращают следующее сообщение:

```
/proc/sys/net/ipv4/conf/all/log_martians:1
/proc/sys/net/ipv4/conf/default/log_martians:1
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить виртуальные машины на запись в журнал пакетов martian IPv4, откройте файл `/etc/sysctl.conf` в текстовом редакторе.
3. Проверьте значения строк, которые начинаются с `net.ipv4.conf`.

Если значение для следующих записей не установлены на 1 или они не существуют, добавьте их в этот файл или обновите существующие записи надлежащим образом.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

4. Сохраните изменения и закройте файл.

Фильтрация обратного тракта IPv4

В целях безопасности рекомендуется настроить на узлах устройства VMware фильтрацию обратного тракта IPv4.

Фильтрация обратного тракта обеспечивает защиту от ложных адресов источников за счет того, что система игнорирует пакеты с адресами источника, которые не имеют маршрута или маршрут которых не указывает на исходный интерфейс. Настройте узлы так, чтобы фильтрация обратного тракта на них использовалась всегда, когда это возможно. В некоторых случаях, в зависимости от роли системы, фильтрация обратного тракта может привести к игнорированию допустимого трафика. Если обнаружится подобная проблема, попробуйте установить менее жесткий режим или отключите фильтрацию обратного тракта.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter | egrep "default|all"` на узлах виртуального устройства VMware, чтобы проверить используется ли на них фильтрация обратного тракта IPv4.

Если на виртуальных машинах используется фильтрация обратного тракта IPv4, результат команды будет следующим:

```
/proc/sys/net/ipv4/conf/all/rp_filter:1
/proc/sys/net/ipv4/conf/default/re_filter:1
```

Если виртуальные машины настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить фильтрацию обратного тракта IPv4 на узлах, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте значения строк, которые начинаются с `net.ipv4.conf`

Если указанных далее записей нет или для них не установлено значение 1, добавьте эти записи в файл или измените их значения соответствующим образом.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

4. Сохраните изменения и закройте файл.

Отклонение переадресации IPv4

Настройте на узлах устройства VMware отклонение переадресации IPv4.

Если в системе настроена IP-передача и данная система не является назначенным маршрутизатором, злоумышленники могут использовать это для обхода системы безопасности сети, указав для передачи данных путь, обходящий фильтрацию на сетевых устройствах. Настройте на узлах виртуального устройства отклонение переадресации IPv4, чтобы защититься от подобной угрозы.

Процедура

1. Выполните команду `# cat /proc/sys/net/ipv4/ip_forward` на узлах устройства VMware, чтобы проверить, отклоняется ли на них переадресация IPv4.

Если для узлов настроено отклонение переадресации IPv4, команда вернет значение 0 для параметра `/proc/sys/net/ipv4/ip_forward`. Если виртуальные машины настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить на узле виртуального устройства отклонение переадресации IPv4, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Найдите такую запись: `net.ipv4.ip_forward=0`. Если указанной записи нет или для нее не установлено нулевое значение, добавьте эту запись или измените ее значение соответствующим образом.
4. Сохраните изменения и закройте файл.

Отклонение переадресации IPv6

В целях безопасности рекомендуется настроить на узлах устройства VMware отклонение переадресации IPv6.

Если в системе настроена IP-передача и данная система не является назначенным маршрутизатором, злоумышленники могут использовать это для обхода системы безопасности сети, указав для передачи данных путь, обходящий фильтрацию на сетевых устройствах. Настройте на узлах виртуального устройства отклонение переадресации IPv6, чтобы защититься от подобной угрозы.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding | egrep "default|all"` на VMware узлах устройства, чтобы проверить, отклоняется ли на них переадресация IPv6.

Если для узлов настроено отклонение переадресации IPv6, результат команды будет таким:

```
/proc/sys/net/ipv6/conf/all/forwarding:0
/proc/sys/net/ipv6/conf/default/forwarding:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить на узле отклонение переадресации IPv6, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте значения строк, которые начинаются с `net.ipv6.conf`

Если указанных далее записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

4. Сохраните внесенные изменения и закройте файл.

Использование Syncookies TCP IPv4

Убедитесь, что компьютеры узла устройств VMware используют Syncookies TCP IPv4.

Синхронная атака TCP может привести к отказу в обслуживании путем заполнения таблицы TCP-соединений системы соединениями в состоянии SYN_RCVD. Технология Syncookies предотвращает отслеживание соединения до получения последующего ACK, проверяя, что инициатор пытается выполнить допустимое подключение и не является источником Flood-атаки. Эта технология не работает полностью совместимым со стандартами способом. Он активируется только при условии Flood-атаки, а также позволяет защитить систему, продолжая обслуживать допустимые запросы.

Процедура

1. Запустите команду `# cat /proc/sys/net/ipv4/tcp_syncookies` на компьютерах узла устройств VMware, чтобы убедиться, что они используют Syncookies TCP IPv4.

Если компьютеры узла настроены на запрет перенаправления IPv4, эта команда вернет значение 1 для `/proc/sys/net/ipv4/tcp_syncookies`. Если виртуальные машины настроены правильно, никаких других действий не требуется.

2. Чтобы настроить виртуальное устройство на использование Syncookies TCP IPv4, откройте `/etc/sysctl.conf` в текстовом редакторе.

3. Найдите такую запись: `net.ipv4.tcp_syncookies=1`.

Если для этой записи в настоящий момент не установлено значение единицы или если она не существует, добавьте запись или измените существующую запись соответственно.

4. Сохраните внесенные изменения и закройте файл.

Отклонение объявлений маршрутизатора IPv6

Настройте для узлов VMware отклонение объявлений маршрутизатора и перенаправлений ICMP, если такие объявления и перенаправления не требуются для работы системы.

Протокол IPv6 позволяет системам настраивать сетевые устройства посредством автоматического применения информации из сети. С точки зрения безопасности настройка важных данных конфигурации вручную является более надежным методом по сравнению с приемом данных из сети без надлежащих проверок.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra | egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них объявления маршрутизатора.

Если для узлов настроено отклонение объявлений маршрутизатора IPv6, команда вернет значение 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra:0
/proc/sys/net/ipv6/conf/default/accept_ra:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить отклонение объявлений маршрутизатора IPv6 на узлах, откройте в текстовом редакторе файл `/etc/sysctl.conf`.

3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните внесенные изменения и закройте файл.

Отклонение вызовов маршрутизатора IPv6

В целях безопасности рекомендуется настроить на узлах устройства VMware отклонение вызовов маршрутизатора IPv6, если иное не требуется для работы системы.

Параметр вызовов маршрутизатора определяет, сколько таких вызовов отправляется при получении интерфейса. Если назначаются статические адреса, в отправке вызовов нет необходимости.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них вызовы маршрутизатора IPv6.

Если для узлов настроено отклонение объявлений маршрутизатора IPv6, результат команды будет таким:

```
/proc/sys/net/ipv6/conf/all/router_solicitations:0
/proc/sys/net/ipv6/conf/default/router_solicitations:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить отклонение вызовов маршрутизатора IPv6 на узлах, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните изменения и закройте файл.

Отклонение предпочтения маршрутизатора IPv6 при вызовах маршрутизатора

Настройте на узлах устройства VMware отклонение вызовов маршрутизатора IPv6, если иное не требуется для работы системы.

Параметр предпочтения маршрутизатора при вызовах определяет предпочтения маршрутизатора. Если назначаются статические адреса, получать сведения о предпочтении маршрутизатора при вызовах не требуется.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref | egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них вызовы маршрутизатора IPv6.

Если для узлов настроено отклонение объявлений маршрутизатора IPv6, результат команды будет таким:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rtr_pref:0
/proc/sys/net/ipv6/conf/default/accept_ra_rtr_pref:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить отклонение вызовов маршрута IPv6 на узлах, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните внесенные изменения и закройте файл.

Отклонение префикса маршрутизатора IPv6

Настройте на узлах устройства VMware отклонение префикса маршрутизатора IPv6, если иное не требуется для работы системы.

Параметр `accept_ra_rinfo` определяет, принимает ли система сведения о префиксе от маршрутизатора. Если назначаются статические адреса, получать сведения о префиксе маршрутизатора не требуется.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rinfo | egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них сведения о префиксе маршрутизатора IPv6.

Если для узлов настроено отклонение объявлений маршрутизатора IPv6, результат команды будет таким:

```
/proc/sys/net/ipv6/conf/all/accept_ra_rinfo:0
/proc/sys/net/ipv6/conf/default/accept_ra_rinfo:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить отклонение сведений о префиксе маршрутизатора IPv6 на узлах, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните изменения и закройте файл.

Отклонение ограничений прыжков в объявлении маршрутизатора IPv6

Настройте для узлов устройства VMware отклонение ограничений прыжков маршрутизатора IPv6, если такие ограничения не требуются.

Параметр `accept_ra_defrtr` определяет, принимает ли система ограничения прыжков из объявления маршрутизатора. При нулевом значении параметра маршрутизатор не сможет изменить ваше стандартное ограничение прыжков IPv6 для исходящих пакетов.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr | egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них ограничения прыжков маршрутизатора IPv6.

Если для узлов настроено отклонение ограничений прыжков маршрутизатора IPv6, команда вернет значение 0.

```
/proc/sys/net/ipv6/conf/all/accept_ra_defrtr:0
/proc/sys/net/ipv6/conf/default/accept_ra_defrtr:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить на узле отклонение ограничений прыжков маршрутизатора IPv6, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните внесенные изменения и закройте файл.

Отклонение настроек автоматической конфигурации в объявлении маршрутизатора IPv6

Настройте для узлов устройства VMware отклонение настроек автоматической конфигурации маршрутизатора IPv6, если такие настройки не требуются.

Параметр `autoconf` определяет, может ли система на основании объявлений маршрутизатора назначить глобальный индивидуальный адрес интерфейсу.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf | egrep "default|all"` на узлах устройства VMware, чтобы проверить, отклоняются ли на них настройки автоматической конфигурации маршрутизатора IPv6.

Если для узлов настроено отклонение настроек автоматической конфигурации маршрутизатора IPv6, команда вернет значение 0.

```
/proc/sys/net/ipv6/conf/all/autoconf:0
/proc/sys/net/ipv6/conf/default/autoconf:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить на узле отклонение настроек автоматической конфигурации маршрутизатора IPv6, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните внесенные изменения и закройте файл.

Отклонение вызовов соседа IPv6

Настройте на узлах устройства VMware отклонение вызовов соседа IPv6, если такие вызовы не требуются.

Параметр `dad_transmits` определяет, сколько вызовов соседа должно отправляться на один адрес (глобальный и link-local) при получении интерфейса для обеспечения уникальности данного адреса в сети.

Процедура

1. Выполните команду `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits | egrep "default|all"` на VMware узлах устройства, чтобы проверить, отклоняются ли на них вызовы соседа IPv6.

Если для узлов настроено отклонение вызовов соседа IPv6, команда вернет значение 0.

```
/proc/sys/net/ipv6/conf/all/dad_transmits:0
/proc/sys/net/ipv6/conf/default/dad_transmits:0
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить на узле отклонение вызовов соседа IPv6, откройте в текстовом редакторе файл `/etc/sysctl.conf`.
3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

Если записей нет или для них не установлены нулевые значения, добавьте эти записи или измените их значения соответствующим образом.

4. Сохраните внесенные изменения и закройте файл.

Ограничение максимального количества адресов IPv6

Убедитесь, что компьютеры узлов устройства VMware ограничивают параметр максимального количества адресов IPv6 до минимума, необходимого для работы системы.

Параметр максимального количества адресов IPv6 определяет количество глобальных одноадресных адресов IPv6, доступных для каждого интерфейса. Количество по умолчанию — 16 адресов, но необходимо задать точное количество статически настроенных глобальных адресов, необходимых для используемой системы.

Процедура

1. Выполните команду `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses | egrep "default|all"` на компьютерах узлов устройства VMware, чтобы убедиться, что они надлежащим образом ограничивают максимальное количество адресов IPv6.

Если компьютеры узлов настроены на ограничение максимального количества адресов IPv6, эта команда вернет значения 1.

```
/proc/sys/net/ipv6/conf/all/max_addresses:1
/proc/sys/net/ipv6/conf/default/max_addresses:1
```

Если узлы настроены правильно, никаких других действий не требуется.

2. Если необходимо настроить максимальное количество адресов IPv6 на компьютерах узлов, откройте файл `/etc/sysctl.conf` в текстовом редакторе.

3. Проверьте указанные далее записи.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

Если записи не существуют или их значения не равны 1, добавьте такие записи или обновите надлежащим образом существующие записи.

4. Сохраните внесенные изменения и закройте файл.

Настройка параметров сети для узла инфраструктуры как услуги

В целях безопасности рекомендуется настроить параметры обмена данными в сети на узле компонента инфраструктуры как услуги VMware в соответствии с требованиями и инструкциями VMware.

Чтобы обеспечить поддержку всех функций vRealize Automation с надлежащим уровнем безопасности, настройте конфигурацию сети для узла инфраструктуры как услуги.

См. раздел [Защита компонента инфраструктуры как услуги](#).

Настройка портов и протоколов

Рекомендуется настроить порты и протоколы для всех устройств и компонентов vRealize Automation в соответствии с руководствами VMware.

Настройте входящие и исходящие порты для компонентов vRealize Automation в соответствии с требованиями к работе критически важных компонентов системы в производственной среде. Отключите все ненужные порты и протоколы. См. раздел *Эталонная архитектура vRealize Automation* в [документации по VMware vRealize Automation](#).

Инструмент «Порты и протоколы»

С помощью средства «Порты и протоколы» можно просматривать информацию о портах для различных продуктов VMware, в том числе для нескольких продуктов одновременно, на одной панели управления. Кроме того, можно экспортировать выбранные данные из этого средства для доступа в автономном режиме. В настоящее время средство «Порты и протоколы» поддерживает следующие решения:

- vSphere;
- vSAN;
- NSX for vSphere;
- vRealize Network Insight;
- vRealize Operations Manager;
- vRealize Automation.

Это средство можно загрузить на сайте <https://ports.vmware.com/>.

Пользовательские порты

В целях безопасности настройте пользовательские порты vRealize Automation в соответствии с инструкциями VMware.

Необходимые порты должны быть доступны только через защищенную сеть.

СЕРВЕР	ПОРТЫ
Устройство vRealize Automation	443, 8443

Порты, необходимые администратору

В целях безопасности рекомендуется настроить порты администратора vRealize Automation в соответствии с инструкциями VMware.

Необходимые порты должны быть доступны только через защищенную сеть.

СЕРВЕР	ПОРТЫ
Сервер vRealize Application Services	5480

Порты устройства vRealize Automation

В целях обеспечения безопасности рекомендуется настроить входящие и исходящие порты для Устройство vRealize Automation в соответствии с инструкциями VMware.

Входящие порты

Настройте минимальное необходимое количество входящих портов для Устройство vRealize Automation.

Настройте дополнительные порты, если это необходимо для конфигурации вашей системы.

Таблица 8-1. Минимальное обязательное количество входящих портов

ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
443	TCP	Доступ к вызовам API и консоли vRealize Automation
8443	TCP	Прокси-сервер VMware Remote Console
5480	TCP	Доступ к интерфейсу управления устройством vRealize Automation.
5488, 5489	TCP	Внутренний. Используется решением Устройство vRealize Automation для обновлений.
5672	TCP	Обмен сообщениями RabbitMQ.
Примечание При кластеризации экземпляров Устройство vRealize Automation, возможно, понадобится настроить открытые порты 4369 и 25672.		
40002	TCP	Требуется для службы vIDM. Защищено брандмауэром от всего внешнего трафика за исключением трафика от других узлов Устройство vRealize Automation при добавлении в конфигурацию высокой доступности.

Если необходимо, настройте дополнительные входящие порты.

Таблица 8-2. Дополнительные входящие порты

ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
22	TCP	(Дополнительно) SSH. В производственной среде отключите службу SSH, прослушивающую порт 22, и закройте порт 22.
80	TCP	(Дополнительно) Перенаправляет на порт 443.

Исходящие порты

Настройте необходимые исходящие порты.

Таблица 8-3. Минимальное обязательное количество исходящих портов

ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
25,587	TCP и UDP	Протокол SMTP для отправки исходящих уведомлений по электронной почте.
53	TCP и UDP	DNS.
67, 68, 546, 547	TCP и UDP	DHCP.
110, 995	TCP и UDP	Протокол POP для получения входящих уведомлений по электронной почте.
143, 993	TCP и UDP	Протокол IMAP для получения входящих уведомлений по электронной почте.
443	TCP	Служба управления инфраструктурой как услуги по протоколу HTTPS.

Если необходимо, настройте дополнительные исходящие порты.

Таблица 8-4. Дополнительные исходящие порты

ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
80	TCP	(Дополнительно) Используется для получения обновлений программного обеспечения. Обновления можно загружать и применять по отдельности.
123	TCP и UDP	(Дополнительно) Используется для подключения непосредственно к NTP вместо использования времени узла.

Средство «Порты и протоколы»

С помощью средства «Порты и протоколы» можно просматривать информацию о портах для различных продуктов VMware, в том числе для нескольких продуктов одновременно, на одной панели управления. Кроме того, можно экспортировать выбранные данные из этого средства для доступа в автономном режиме. В настоящее время средство «Порты и протоколы» поддерживает следующие решения:

- vSphere;
- vSAN;
- NSX for vSphere;
- vRealize Network Insight;

- vRealize Operations Manager;
- vRealize Automation.

Эти средства доступны на портале <https://ports.vmware.com/>.

Порты инфраструктуры как услуги

Рекомендуется настроить входящие и исходящие порты для компонентов инфраструктуры как услуги (IaaS) в соответствии с руководствами VMware.

Входящие порты

Настройте минимальное количество требуемых входящих портов для компонентов инфраструктуры как услуги.

Таблица 8-5. Минимальное обязательное количество входящих портов

КОМПОНЕНТ	ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
Manager Service	443	TCP	Обмен данными с компонентами инфраструктуры как услуги и устройством vRealize Automation по протоколу HTTPS. На любых узлах виртуализации, которыми управляют прокси-агенты, также должен быть открыт для входящего трафика TCP-порт 443

Исходящие порты

Настройте минимальное количество требуемых исходящих портов для компонентов инфраструктуры как услуги.

Таблица 8-6. Минимальное обязательное количество исходящих портов

КОМПОНЕНТ	ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
Все	53	TCP и UDP	DNS.
Все		TCP и UDP	DHCP.
Manager Service	443	TCP	Обмен данными с устройством vRealize Automation по протоколу HTTPS.
Веб-сайт	443	TCP	Обмен данными со службой диспетчера по протоколу HTTPS.
Диспетчеры Distributed Execution Manager	443	TCP	Обмен данными со службой диспетчера по протоколу HTTPS.
Прокси-агенты	443	TCP	Обмен данными с компонентом «Служба диспетчера» и узлами виртуализации по протоколу HTTPS.
Гостевой агент	443	TCP	Обмен данными со службой диспетчера по протоколу HTTPS.
Служба диспетчера, веб- сайт	1433	TCP	MSSQL.

При необходимости настройте дополнительные исходящие порты.

Таблица 8-7. Дополнительные исходящие порты

КОМПОНЕНТ	ПОРТ	ПРОТОКОЛ	КОММЕНТАРИИ
Все	123	TCP и UDP	NTP не является обязательным.

Аудит и ведение журнала

В целях безопасности рекомендуется настроить аудит и ведение журнала в системе vRealize Automation в соответствии с инструкциями VMware.

При удаленном ведении журнала на специальном центральном узле обеспечивается безопасное хранение файлов журнала. Собирая файлы журнала на центральном узле, вы можете контролировать среду с помощью единого инструмента. Также можно выполнять общий анализ и поиск признаков угроз, например согласованных атак на нескольких объектах в рамках инфраструктуры. Ведение журнала на едином защищенном сервере поможет избежать нежелательных действий с журналом и в течение длительного времени сохранять необходимые записи аудита.

Обеспечение безопасности сервера удаленного ведения журнала

После взлома системы защиты на узле злоумышленники часто пытаются найти и изменить файлы журнала, чтобы скрыть свои действия и сохранить полученный контроль над системой, оставшись незамеченными. Для предотвращения незаконных изменений журнала следует надлежащим образом защитить сервер удаленного ведения журнала.

Использование авторизованного NTP-сервера

На всех узлах должен использоваться один и тот же источник относительного времени (с учетом смещения вследствие локализации), соответствующий одобренному стандарту времени, например всемирному координированному времени (Coordinated Universal Time, UTC). Правильно организованное использование источников времени позволяет быстро отслеживать и соотносить между собой действия злоумышленников при проверке соответствующих файлов журнала. При неправильных настройках времени усложняются проверка и сопоставление файлов журнала с целью выявления атак, а аудит дает неточные результаты.

Используйте по крайней мере три NTP-сервера на основе внешних источников времени или настройте несколько локальных NTP-серверов в доверенной сети, которые будут получать данные времени как минимум от трех внешних источников времени.