Наилучшие практики для безопасной установки Zabbix

Обзор

В этом разделе содержатся рекомендации, которые следует соблюдать для того, чтобы настроить Zabbix безопасным образом.

Практики, описанные здесь, не требуются для работы Zabbix. Они рекомендуются для повышения безопасности системы.

Принцип минимальных привилегий

Подход назначения минимальных привилегий необходимо использовать для Zabbix на постоянной основе. Этот принцип означает, что аккаунты пользователей (в Zabbix веб-интерфейсе) и пользователь процессов (для Zabbix сервера/прокси или агента) должны иметь только те привилегии, которые им необходимы для выполнения намеченных функций. Другими словами, аккаунты пользователей должны всегда иметь как можно меньше привилегий насколько это возможно.

Предоставление дополнительных прав пользователю 'zabbix' даст возможность доступа к файлам конфигурации и выполнению операций, которые могут поставить под угрозу общую безопасность инфраструктуры.

При реализации принципа минимальных привилегий для аккаунтов пользователей необходимо принимать во внимание Zabbix типы пользователей в веб-интерфейсе Zabbix. Важно понимать, что хотя тип пользователя "Zabbix Администратор" имеет меньше привилегий чем тип пользователя "Zabbix Супер-Администратор", у него также имеются административные права, которые позволяют управлять конфигурацией и выполнять пользовательские скрипты.

Некоторая информация доступна даже непривилигерованным пользователям. Например, тогда как *Администрирование → Скрипты* недоступно для не-Супер Администраторов, сами скрипты доступны для получения при помощи Zabbix API. Необходимо использовать ограничение прав доступа к скриптам и избежание добавления конфиденциальных данных (такой как, учётные данные и т.д.), чтобы исключить раскрытие конфиденциальной информации доступной в глобальных скриптах.

Защищённый пользователь для Zabbix агента

В конфигурации по умолчанию процессы Zabbix сервера и Zabbix агента делят одного 'zabbix' пользователя. Если вы убедиться, что агент не сможет получить доступ к конфиденциальной информации из конфигурации сервера (например, данные подключения в базе данных), агента необходимо запускать из под другого пользователя:

1. Создайте защищённого пользователя
2. Укажите этого пользователя в файле конфигурации агента (параметр 'User')
3. Перезапустите агента с правами администратора. Привилегии администратора сбросятся на указанного пользователя.

UTF-8 кодировка

UTF-8 является единственной кодировкой, которая поддерживается Zabbix. Она, как известно, работает без каких-либо проблем с безопасностью. Пользователи должны знать, что существуют известные проблемы с безопасностью при использовании некоторых других кодировок.

Настройка SSL для Zabbix веб-интерфейса

На RHEL/Centos, установите пакет mod_ssl:

```
yum install mod_ssl
```

Создайте папку для SSL ключей:

```
mkdir -p /etc/httpd/ssl/private
chmod 700 /etc/httpd/ssl/private
```

Создайте SSL сертификат:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/httpd/ssl/private/apache-selfsigned.key -out /etc/httpd/ssl/apache-
selfsigned.crt
```

Заполните подсказки соответствующим образом. Самая важная строка здесь, которая запрашивает Common Name. Вам необходимо указать имя домена, которое вы хотите связать с вашим сервером. Вместо него вы можете указать публичный IP адрес, если у вас отсутствует имя домена. В этой статье мы будем использовать *example.com*.

```
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:
```

Измените конфигурацию Apache SSL:

```
/etc/httpd/conf.d/ssl.conf
```

```
DocumentRoot "/usr/share/zabbix"
ServerName example.com:443
SSLCertificateFile /etc/httpd/ssl/apache-selfsigned.crt
SSLCertificateKeyFile /etc/httpd/ssl/private/apache-selfsigned.key
```

Перезапустите сервис Apache, чтобы применить изменения:

```
systemctl restart httpd.service
```

Включение Zabbix в корневом каталоге URL

Добавьте виртуальный хост в конфигурацию Apache и задайте постоянную переадресацию для корневого каналога на Zabbix SSL URL. Не забудьте заменить *example.com* на актуальное имя сервера.

```
/etc/httpd/conf/httpd.conf
```

```
#Добавьте строки

<VirtualHost *:*>
    ServerName example.com
    Redirect permanent / http://example.com
</VirtualHost>
```

Перезапустите сервис Apache, чтобы применить изменения:

```
systemctl restart httpd.service
```

Включение HTTP Strict Transport Security (HSTS) на веб-сервере

HSTS применяется Zabbix веб-интерфейсом в версиях 3.0.13 - 3.0.24.

Для всех других версий, чтобы защитить Zabbix веб-интерфейс от атак понижения протокола, мы рекомендуем включить на веб-сервере HSTS политику.

Например, чтобы включить HSTS политику для вашего Zabbix веб-интерфейса в конфигурации Apache:

```
/etc/httpd/conf/httpd.conf
```

добавьте следующую директиву к конфигурации вашего виртуального хоста:

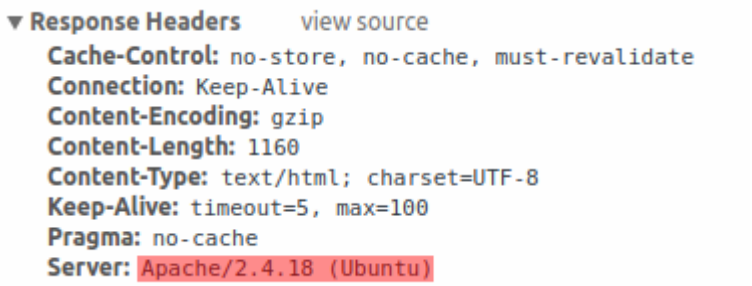
```
<VirtualHost *:443>
   Header set Strict-Transport-Security "max-age=31536000"
</VirtualHost>
```

Перезапустите сервис Apache, чтобы применить изменения:

```
systemctl restart httpd.service
```

Отключение отображения информации о веб-сервере

Рекомендуется отключить все подписи веб-сервера, как часть процесса по улучшению защищенности веб-сервера. По умолчанию веб-сервер раскрывает подпись программного обеспечения:



Эту подпись можно отключить, добавив две строки в файл конфигурации Apache (используется как пример):

```
ServerSignature Off
ServerTokens Prod
```

Подпись PHP (Заголовок X-Powered-By HTTP) можно отключить, изменив файл конфигурации php.ini (подпись отключена по умолчанию):

```
expose_php = Off
```

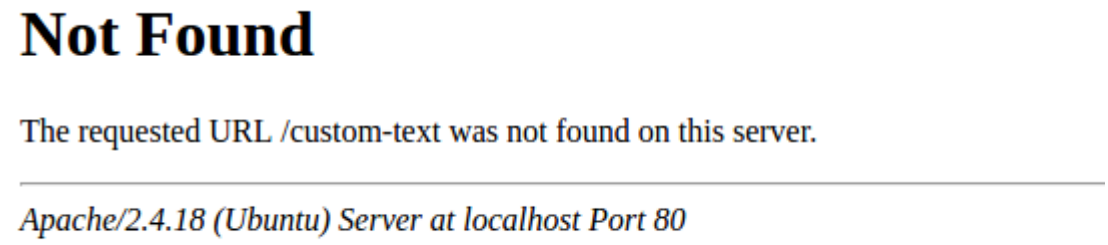
Чтобы изменения файлов конфигурации вступили в силу, необходимо перезапустить веб-сервер.

Дополнительный уровень безопасности можно достичь, используя mod_security (пакет libapache2-mod-security2) с Apache. mod_security позволяет совсем удалить подпись сервера вместо удаления лишь версии из подписи сервера. Подпись можно изменить на любое значение, исправив “SecServerSignature” на любое желаемое значение, после установки mod_security.

Пожалуйста, обратитесь к документации по вашему веб-серверу для того, чтобы узнать как удалять/изменять подписи к программному обеспечанию.

Отключение страниц ошибок по умолчанию веб-сервера

Рекомендуется отключить страницы ошибок по умолчанию, чтобы избежать раскрытия информации. По умолчанию веб-сервер использует встроенные страницы ошибок:

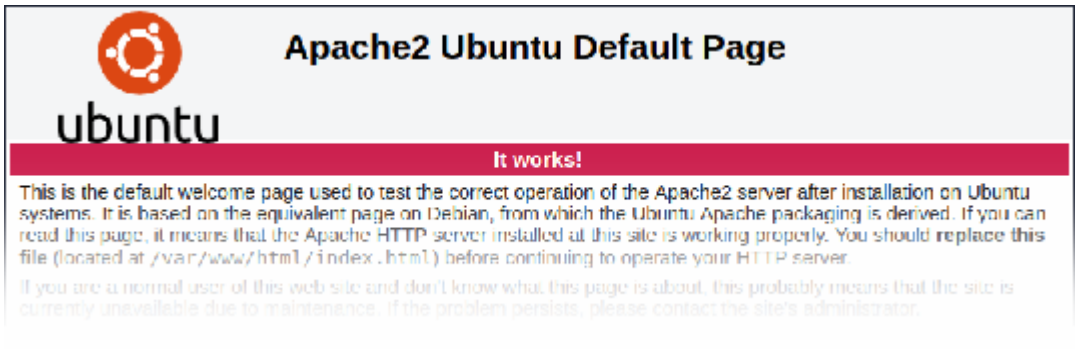


Страницы ошибок по умолчанию необходимо заменить/удалить, как часть процесса по улучшению защищенности веб-сервера. Можно использовать директиву “ErrorDocument”, чтобы задать пользовательскую страницу/текст веб-серверу Apache (используется как пример).

Пожалуйста, обратитесь к документации по вашему веб-серверу для того, чтобы узнать как заменять/удалять страницы ошибок по умолчанию.

Удаление тестовой страницы с веб-сервера

Рекомендуется удалить тестовую страницу веб-сервера, чтобы избежать раскрытия информации. По умолчанию, корневой каталог веб-сервера содержит тестовую страницу с именем index.html (Apache2 на Ubuntu используется как пример):



Тестовую страницу необходимо удалить или сделать недоступной, как часть процесса по улучшению защищенности веб-сервера.