

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.

Защищённый пользователь для Zabbix агента

В конфигурации по умолчанию процессы Zabbix сервера и Zabbix агента делят одного 'zabbix' пользователя. Если вы убедитесь, 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 канала 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
```

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:

```
▼ Response Headers    view source
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1160
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.18 (Ubuntu)
```

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 обеспечению.

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:

Not Found

The requested URL /custom-text was not found on this server.

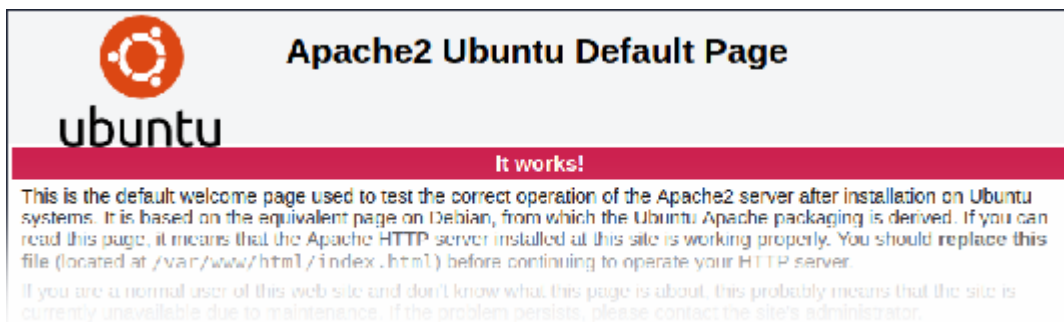
Apache/2.4.18 (Ubuntu) Server at localhost Port 80

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.

From: <https://www.zabbix.com/documentation/3.4/> - Zabbix Documentation 3.4

Permanent link: https://www.zabbix.com/documentation/3.4/ru/manual/installation/requirements/best_practices

Last update: 2019/11/28 05:46

