# Лучшие практики по безопасной инсталляции Zabbix

## Обзор

Этот раздел содержит лучшие практики, которые необходимо соблюсти для настройки Zabbix с учётом аспектов безопасности.

Описанные здесь практики не требуются для нормального функционирования Zabbix. Они рекомендуются для более лучшей безопасности системы.

## Надежный пользователь для Zabbix агента

При использовании конфигурации по умолчанию процессы Zabbix сервера и Zabbix агента используют одного пользователя 'zabbix'. Если вы хотите быть уверенными, что агент не сможет получить доступ к конфиденциальным деталям о конфигурации сервера (например, информацию о доступе к базе данных), тогда агента необходимо запускать из под другого пользователя:

1. Создайте надежного пользователя
2. Укажите этого пользователя в файле конфигурации (параметр 'User') агента.
3. Перезапустите агента с правами администратора. Привилегии будут сброшены на привилегии заданного пользователя.

## Настройка SSL для Zabbix веб-интерфейса

На RHEL/Centos, установите пакет mod_ssl:

```
yum install mod_ssl
```

Создайте директорию для SSL ключей:

```
mkdir /etc/httpd/ssl
```

Добавьте настройки для SSL инсталляции:

```
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) []:localhost
Email Address []:
```

Измените конфигурацию Apache SSL:

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

```
DocumentRoot "/usr/share/zabbix"
ServerName localhost:443
SSLCertificateFile /etc/httpd/ssl/apache.crt
SSLCertificateKeyFile /etc/httpd/ssl/apache.key
```

Перезапустите сервис Apache, чтобы изменения вступили в силу:

```
systemctl restart httpd.service
```

#### Включение Zabbix корневого каталога URL адреса

Добавьте виртуальный хост в конфигурацию Apache и задайте постоянную переадресацию с корневого каталога на Zabbix SSL URL. Замените *localhost* на актуальное имя сервера.

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

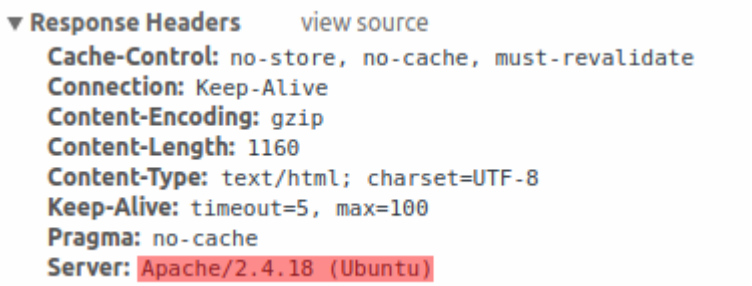
```
#Добавьте строки

<VirtualHost *:*>
    ServerName localhost
    Redirect permanent / http://localhost
</VirtualHost>
```

Перезапустите сервис Apache, чтобы изменения вступили в силу:

```
systemctl restart httpd.service
```

#### Отключение отображения информации о веб-сервере

Рекомендуется отключить все подписи веб-сервера, как часть упрощения работы процесса веб-сервера. По умолчанию веб-сервер отображает подпись о программном обеспечении:




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

```
ServerSignature Off
```

```
ServerTokens Prod
```

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

```
expose_php = Off
```

Необходимо перезапустить веб-сервер, чтобы изменения в файлах конфигурации вступили в силу.

Можно достичь дополнительный уровень безопасности использовав mod_security (пакет libapache2-mod-security2) с Apache. Модуль mod_security позволяет удалить подпись сервера вместо удаления лишь одной версии из подписи сервера. После установки mod_security подпись можно изменить на любое значение, изменив “SecServerSignature” на любое желаемое значение.

Пожалуйста, обратитесь к документации по вашему веб-серверу, чтобы узнать каким образом удалять/менять подписи о программном обеспечении.

#### Отключение страниц ошибок веб-сервера по умолчанию

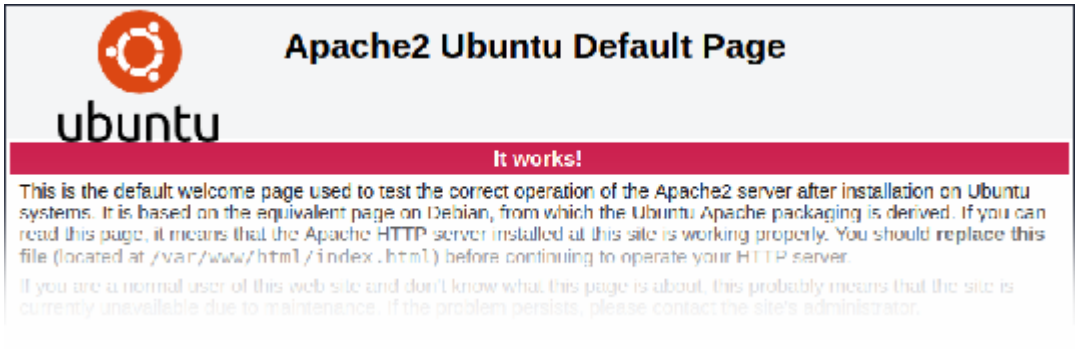
Рекомендуется отключить страницы ошибок по умолчанию, чтобы избежать раскрытия информации. По умолчанию веб-сервер использует встроенные страницы ошибок:


Страницы ошибок по умолчанию необходимо заменить/удалить, как часть упрощения работы процесса веб-сервера. Можно использовать директиву “ErrorDocument”, чтобы задать пользовательскую страницу об ошибке или текст для веб-сервера Apache (используется как пример).

Пожалуйста, обратитесь к документации по вашему веб-серверу, чтобы узнать каким образом заменить/удалить страницы ошибок по умолчанию.

#### Удаление тестовой страницы веб-сервера

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




Тестовую страницу необходимо удалить или сделать недоступной, как часть упрощения работы процесса веб-сервера.