安全设置 Zabbix 的最佳实践

概述

本章节包含为了以安全的方式设置 Zabbix 应遵守的最佳实践。

Zabbix 的功能不依赖于此处的实践。但建议使用它们以提高系统的安全性。

Zabbix agent 的安全用户

在默认的配置中，Zabbix server 和 Zabbix agent 进程共享一个“zabbix”用户。 如果您希望确保 Zabbix agent 无法访问 Zabbix server 配置中的敏感详细信息（例如，数据库登录信息），则应以不同的用户身份运行 Zabbix agent。

1. 创建一个安全用户；
1. 在 Zabbix agent 的 配置文件 中指定此用户（修改 'User' parameter）；
1. 以拥有管理员权限的用户重启 Zabbix agent。之后，此权限将赋予给先前指定的用户。

为 Zabbix 前端设置 SSL

在 RHEL/Centos 操作系统上，安装 mod_ssl 包：

```
yum install mod_ssl
```

为 SSL keys 创建目录：

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

创建 SSL 证书：

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

下面提示内容适当填写。 最重要的一行是请求 Common Name 的行。 您需要输入要与服务器关联的域名。 如果您没有域名，则可以输入公共IP地址。 下面将使用 *example.com*。

```
Country Name (两个字母) [XX]:
State or Province Name (全名) []:
Locality Name (eg, city) [默认的城市]:
Organization Name (eg, company) [默认的公司名]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:
```

编辑 Apache SSL 配置：

```
/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
```

重启 Apache 服务使以上修改的配置生效：

```
systemctl restart httpd.service
```

在 URL 的根目录上启用 Zabbix

将虚拟主机添加到 Apache 配置，并将文档根目录的永久重定向设置为 Zabbix SSL URL。不要忘记将 *example.com* 替换为服务器的实际名称。

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

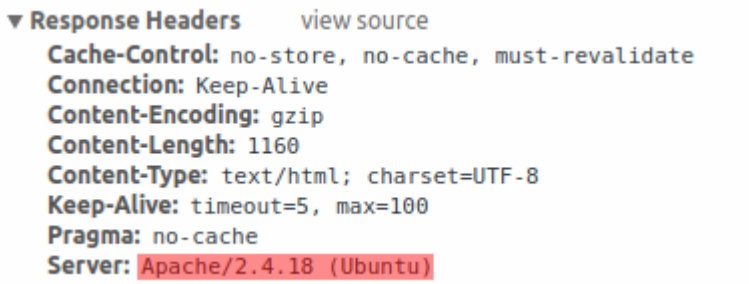
```
#Add lines

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

重启 Apache 服务使以上修改的配置生效：

```
systemctl restart httpd.service
```

禁用曝光的 Web 服务器信息

建议在 Web 服务器强化过程中禁用所有 Web 服务器签名。 默认情况下，Web 服务器正在公开软件签名：



可以通过向 Apache（用作示例）配置文件添加两行来禁用签名：

```
ServerSignature Off
ServerTokens Prod
```

可以通过更改 php.ini 配置文件来禁用 PHP 签名（X-Powered-By HTTP header，默认情况下禁用签名）：

```
expose_php = Off
```

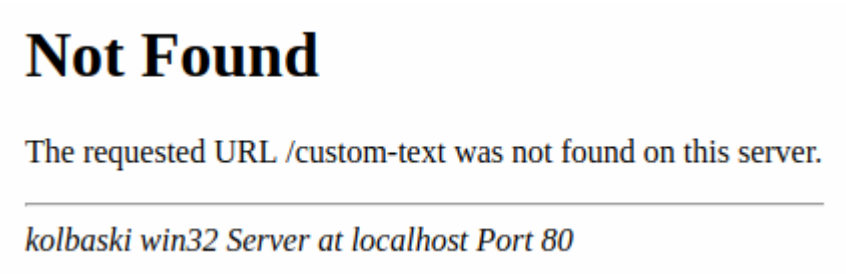
若要应用配置文件更改，需要重新启动 Web 服务器。

通过在 Apache中 使用 mod_security（ libapache2-mod-security2）可以实现额外的安全级别（ mod_security 允许删除服务器签名，而不是仅仅从服务器签名中删除版本。 通过在安装 mod_security 之后将“SecServerSignature”更改为任何所需的值，可以将签名更改为任何值。

请参阅 Web 服务器的文档以获取有关如何删除/更改软件签名的帮助。

Disabling default web server error pages

It is recommended to disable default error pages to avoid information exposure. Web server is using built-in error pages by default:

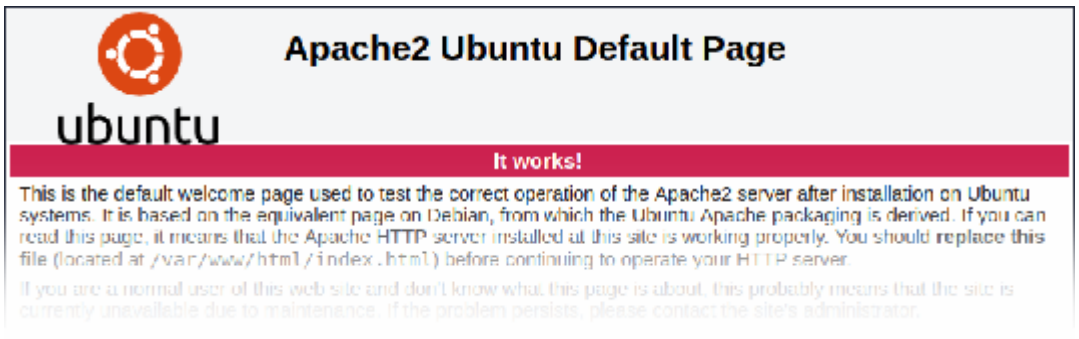


Default error pages should be replaced/removed as part of the web server hardening process. The “ErrorDocument” directive can be used to define a custom error page/text for Apache web server (used as an example).

Please refer to documentation of your web server to find help on how to replace/remove default error pages.

删除 Web 服务器的测试页面

建议删除 Web 服务器测试页以避免信息泄露。 默认情况下，Web 服务器的 webroot 包含一个名为 index.html 的测试页（以Ubuntu上的 Apache2 为例）：



应删除测试页面，或者应将其作为Web服务器强化过程的一部分使用。