ООО «СОВРЕМЕННЫЕ АЛГОРИТМЫ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Email Security Solution

ИНСТРУКЦИЯ ПО УСТАНОВКЕ

На 10 листах

2024

Подготовка к установке

1. Установите обновления Linux, для установки ESS требуется работоспособный DNF/APT с доступом к репозиториям дистрибутива

```
dnf update -y
```

или

```
apt update && apt -y dist-upgrade
```

2. Настройте на сервере разрешаемое извне имя. Например почтовый домен myorg.ru Имя сервера ess.myorg.ru Имя сервера и домен не должны совпадать.

```
hostnamectl set-hostname ess.myorg.ru
```

добавьте его в `/etc/hosts`

3. Отключите swap-файл в `/etc/fstab`

4. Распакуйте архив `ESS.tar`:

```
tar -xf ESS.tar -C /home/
```

5. Для тестовой эксплуатации будет достаточным корневой раздел размером **10 ГБ**.

Для продуктива примонтируйте два тома достаточного объема

- `/home/ess/volumes/vol01`
- `/var/lib/elasticsearch/`

6. Перед запуском скрипта автоконфигурации в каталоге `/home/ess/conf/ssl/` уже должен быть сгенерирован SSL-сертификат

`key` - приватный ключ в Base64 кодировке (рекомендуется EC, допускается RSA)

`fullchain` - цепочка сертификатов в Base64 кодировке

они будут перемещены в `/etc/nginx/`

Создание сертификатов с помощью Lets Encrypt

Существует множество acme-клиентов, данный пример использует https://github.com/acmesh-official/acme.sh

Устанавливаем, выбираем провайдера letsencrypt и регистрируемся, указав свой email.

```
curl https://get.acme.sh | sh
~/.acme.sh/acme.sh --set-default-ca --server letsencrypt
~/.acme.sh/acme.sh --register-account -m your@domain.ru
```

Запрос сертификата:

```
~/.acme.sh/acme.sh --issue --standalone -d ess.myorg.ru
```

Создаем в каталоге `/home/ess/conf/ssl/` нужные файлы

```
cd ~/.acme.sh/ess.myorg.ru_ecc
cat ess.myorg.ru.key > /home/ess/conf/ssl/key
cat fullchain.cer > /home/ess/conf/ssl/fullchain
```

Создание сертификатов в окружении Active Directory

На этом этапе потребуется консультация местных ИТ-специалистов
PKI может быть сайтом в интранет, сертификаты могут выписываться вручную.

Создаем приватный ключ

```
cd /home/ess/conf/ssl/
openssl ecparam -genkey -name prime256v1 -noout -out key
```

или

```
openssl genrsa -out key 2048
```

Создаем CSR (запрос на генерацию сертификата)

```
openssl req -new -key key -out server.csr -sha256
```

Сохраняем из PKI два файла в формате PEM (BASE64):

- корневой сертификат

- цепочку сертификатов

```
openssl pkcs7 -print_certs -in certnew.p7b  -out fullchain
cp CA.pem /etc/pki/ca-trust/source/anchors/
update-ca-trust enable
```

Внешняя терминация SSL (балансировщик)

Настроить балансировщик и перед тем как продолжить установить переменную NOSSL

```
export NOSSL=1
```

Установка ESS

Запустить настройку, указав параметром пароль для Elasticsearch, Prometheus и Keycloak.

```
bash /home/ess/INSTALL/setup_RedHat.sh thisISmyPASSW00RD
```

или

```
bash /home/ess/INSTALL/setup_Debian.sh thisISmyPASSW00RD
```

Если скрипт завершился, не выдав `SETUP FINISHED OK`, нужно исправить проблему и перезапустить оставшуюся часть скрипта.

После установки

Настоятельно рекомендуется настроить синхронизацию парсера с AD. В файле /home/ess/conf/parser.json прописать как минимум один LDAP-сервер, например

```
"ldap": [ { "store": "/etc/pki/java/cacerts", "host": "ldap.myorg.ru", "port": 3269,
"user": "ssouser@myorg.ru", "pass": "ssopass", "root": "DC=myorg,DC=ru" } ]
```

После чего ESS будет заполнит адресную книгу.

ESS поддерживает сквозную авторизацию в AD (SSO) посредством Keycloak. Нужно создать техническую учетную запись в домене и получить в ИТ-службе keytab-файл.

Установить пакеты в ОС

```
dnf install krb5-server krb5-workstation
```

Настраиваем файл /etc/krb5.conf

` [libdefaults] default_realm = MYORG.RU dns_lookup_realm = false dns_lookup_kdc = true ticket_lifetime = 24h renew_lifetime = 7d forwardable = true allow_weak_crypto = true

[realms] MYORG.RU = { kdc = 10.2.2.2 admin_server = 10.2.2.2 default_domain = myorg.ru }

[domain_realm]
.corp.suek.ru = MYORG.RU corp.suek.ru = MYORG.RU `

Зайти в консоль Keycloak под УЗ adm и паролем, указанным при установке ESS https://ess.myorg.ru/kc/ в realm ESS зайти в раздел User federation Нажать Add new provider, Kerberos Заполнить realm, principal и путь до keytab-файла. После чего можно заходить в ESS под доменными УЗ. Чтобы присвоить учетной записи роли, требуется предварительно войти под ней в ESS.

Для корректной работы скоринга, ESS должен различать локальную и внешнюю почту.
Для этого в конфиге **/home/ess/conf/parser.json** пропишите локальные домены почтовой системы.
Можно указать только основной домен, не перечисляя все поддомены. Например:

```
"local_domains": [ "myorg.ru", "anotherorg.com.br", "myorg-msk.ru" ]
```

mail.myorg.ru и ess.myorg-msk.ru будут распознаны.

Скрипт настройки создает следующие учётные записи:

Учётная запись	**Пароль учётной записи**	**Назначение учётной записи**
initial@user.me	Hello	пользовательская УЗ
service@account.admin	H5a-jRa-D5t-QqM	сервисная УЗ для обновления паролей через личный кабинет на сайте ESS
adm	указанный при установке	УЗ администратора в Keycloak, Elasticsearch, Prometheus

Настоятельно рекомендуется сменить пароли по умолчанию после установки.

Смена пароля учётной записи initial@user.me осуществляется в личном кабинете ESS.

Смена паролей к учётным записям adm и service@account.admin производится в Keycloak
https://myhost.myorg.mydomain/kc/
Пользователь: adm
Пароль: указанный при установке

После смены пароля учётной записи service@account.admin необходимо отредактировать параметр `keycloak.admin.password` в файле конфигурации `/home/ess/conf/backend.properties` и перезапустить сервис командой

```
systemctl restart ess_backend
```

Настройка почтового сервера MS Exchange для работы с ESS

После установки для работы ESS необходимо дополнительно настроить почтовый сервер MS Exchange.

Настройка ведения журнала (Exchange 2013/2016/2019)

1. Войдите в Exchange Control Panel, открыв браузер по адресу https://[exchangeipaddress]/ecp.
2. Нажмите "Compliance management" в левом меню.
3. Нажмите "Journal rules" в верхнем правом меню.
4. Щелкните значок +.
5. Введите название журнала в поле "Name".
6. В поле "If the message is sent to or received from..." выберите "Apply to all messages".
7. В поле с надписью "Journal the following messages.." выберите "All messages".
8. В поле "Send journal reports to field" введите archive@myhost.myorg.mydomain (замените myhost.myorg.mydomain на полное доменное имя вашего сервера ESS).
9. Нажмите Save, чтобы внести изменения.
10. При появлении сообщения: "Do you want this rule to apply to all future messages" нажмите "Accept".

Создание Send Connector

1. Выберите "Mail Flow", а затем "Send Connectors".
2. Нажмите +, чтобы добавить новый Send Connector.
3. Введите "ESS" в поле "Name".
4. Выберите "Custom" для параметра "Type".
5. Нажмите Next.
6. В разделе "Network settings" выберите "Route mail to smart host".
7. Нажмите +, чтобы добавить новый Smart host.
8. Введите полное доменное имя сервера ESS, (например, myhost.myorg.mydomain). Нажмите Save.
9. Новый хост должен быть указан в разделе Smart host в окне New Send Connector. Нажмите Next.
10. Выберите "None" для параметра "Smart host authentication option". Нажмите Next.
11. Нажмите +, чтобы добавить новое адресное пространство. Введите полное доменное имя (FQDN) сервера ESS. Нажмите Next.
12. Нажмите +. Во всплывающем диалоговом окне выберите исходный сервер Exchange, затем нажмите "Add". Нажмите "OK".
13. Нажмите Finish.
14. Откройте командную консоль Exchange. И выполните команду: `Set-SendConnector "ESS" -Port 10025` для смены SMTP порта.

Настройка максимального размера сообщения

По умолчанию максимальный размер отправляемого сообщения для Send Connector составляет 10 МБ. Это недостаточно для большинства приложений для ведения журналов.

Для изменения этого параметра:

1. Откройте командную консоль Exchange.
2. Введите следующую команду, чтобы установить максимальный размер отправляемого сообщения: `Set-SendConnector "ESS" -MaxMessageSize "100 MB"`.
3. Введите следующую команду, чтобы убедиться, что максимальный размер отправляемого сообщения составляет 100 МБ: `Get-SendConnector "ESS" |fl MaxMessageSize`.

Параметры преобразования формата TNEF и кодировка по умолчанию

Для корректной работы ESS необходимо отключить использование формата TNEF для всех сообщений, отправляемых в удаленный домен. Для этого выполните следующую команду PowerShell:

```
C:\Windows\system32>Set-remotedomain default -TNEFEnabled $false
```

Необходимо в качестве кодировки по умолчанию установить UTF-8. Выполните следующие команды PowerShell:

```
C:\Windows\system32>Set-remotedomain default -NonMimeCharacterSet utf-8
```

```
C:\Windows\system32>Set-remotedomain default -CharacterSet utf-8
```

Настройка аутентификации входящих сообщений электронной почты в Exchange Server 2013/2016/2019

Для работы антифишингового модуля ESS необходимо наличие заголовка Authentication-Result во входящих сообщениях электронной почты, который предназначен для отображения результатов проверка и аутентификация DKIM/SPF/DMARC. Чтобы включить проверку DKIM/SPF/DMARC необходимо установить плагин DKIM на сервер.

Установка плагина DKIM в Exchange Server 2013/2016/2019

Загрузите модуль DKIM по ссылке emailarchitect

После завершения установки рекомендуется перейти в `Control -> PanelAdministrative -> ToolsServices` и проверить, запущены ли «**Microsoft Exchange Transport Service**» и «**Microsoft Exchange Mail Submission Service**». Если эти службы не работают, запустите их.

По умолчанию модуль DKIM после завершения установки включает только агент исходящего транспорта, поэтому вам необходимо включить агент входящего транспорта DKIM вручную.

Включение агента входящего транспорта DKIM

Откройте консоль управления Exchange и введите:

```
enable-transportagent "EA Dkim Inbound Agent"
get-transportagent
```

Для применения изменений перезапустите «**Microsoft Exchange Transport Service**»:

```
Restart-Service "MSExchangeTransport"
```

Каждый раз после выполнения обновления или переустановки агента Dkim необходимо заново включать агент входящего транспорта и снова перезапускать «Microsoft Transport Service».

Файл конфигурации и первый тест

Файл конфигурации в формате XML находится в `installation path\DkimInboundAgent.dll.config`, путь установки по умолчанию — `C:\Program Files(x86)\EAExchDomainKeys`.

Чтобы проверить, работает ли агент входящего транспорта, измените в файле конфигурации:

```
<add key ="logLevel" value="OnlyError"/>
```

на:

```
<add key ="logLevel" value="FullDebug"/>
```

затем отправьте тестовое письмо из-за пределов домена, так как внутренние сообщения не будут запускать агент транспорта.

Полный журнал отладки будет находиться в `installation path\log\YYYYDDMM.inbound.txt`

Удаление ESS

Для полного удаления Elasticsearch, Postgresql, Nginx и ESS запустите скрипт и подтвердите удаление символом Y

```
/home/ess/INSTALL/uninstall.sh
```