Сопроводительная документация по развертыванию Программы для ЭВМ «Система управления межсервисной идентификацией»

На 9 листах

ООО «ЭйТи Консалтинг»

2023 г.

СОДЕРЖАНИЕ

1 Общие положения

1.1 Полное наименование Программы для ЭВМ, обозначение

Полное наименование Программы для ЭВМ: Программа для ЭВМ «Система управления межсервисной идентификацией»

Краткое наименование (обозначение) системы: СУМИ, или Система.

1.2 Разработчик Системы

Полное наименование: Общество с ограниченной ответственностью «Эдвансед Трансформейшн Консалтинг»

Сокращенное наименование: ООО «ЭйТи Консалтинг»

1.3 Назначение документа

Настоящий документ входит в комплект эксплуатационной документации по Системе управления межсервисной идентификацией и предназначен для пользователей Системы.

2 Описание требований

2.1 Минимальные аппаратные требования

Количество рабочих станций	10 агентов	100 агентов	1000 агентов	5000 агентов
10	2U, 1 ядро, 1 ГБ оперативной памяти	2U, 2 ядра, 2 ГБ оперативной памяти	2U, 4 ядра, 4 ГБ оперативной памяти	2U, 8 ядер, 8 ГБ оперативной памяти
100	2U, 2 ядра, 2 ГБ оперативной памяти	2U, 2 ядра, 2 ГБ оперативной памяти	2U, 8 ядер, 8 ГБ оперативной памяти	2U, 16 ядер, 16 ГБ оперативной памяти
1000	2U, 16 ядер, 8 ГБ оперативной памяти	2U, 16 ядер, 8 ГБ оперативной памяти	2U, 16 ядер, 8 ГБ оперативной памяти	4U, 16 ядер, 8 ГБ оперативной памяти
10000	4U, 16 ядер, 16 ГБ оперативной памяти	4U, 16 ядер, 16 ГБ оперативной памяти	4U, 16 ядер, 16 ГБ оперативной памяти	8U, 16 ядер, 16 ГБ оперативной памяти

2.2 Программное обеспечение серверов

Операционная система Astra Linux

СУБД «PostgreSQL»

Технологии контейнерной виртуализации Docker

Kubernetes

3 Комплект поставки

В комплект поставки входит:

1. СУМИ агент
2. СУМИ сервер

4 Развертывание

Команды запускаются через обычную учетную запись пользователя, или пользователя с правами root.

Выполните следующую команду, чтобы загрузить и распаковать готовые исполняемые файлы СУМИ сервер и СУМИ агент, а также примеры файлов конфигурации в каталоге spire-1.6.3

```
$ curl -s -N -L
https://github.com/spiffe/spire/releases/download/v1.6.3/spire-1.6.3-
linux-x86_64-glibc.tar.gz | tar xz
```

4.1. Запуск СУМИ сервера

СУМИ сервер управляет удостоверениями и выдает их. Необходимо использовать предоставленный пример файла конфигурации для запуска сервера из каталога, созданного на предыдущем шаге:

```
$ bin/spire-server run -config conf/server/server.conf &

...

INFO[0000] Starting TCP server   address="127.0.0.1:8081"
subsystem_name=endpoints
```

Убедиться в работе сервера:

```
$ bin/spire-server healthcheck

Server is healthy.
```

4.2. Создание токена присоединения для идентификации агента на сервере

Токен — это один из многих доступных методов аттестации агента. Это одноразовый предварительно общий ключ, который аутентифицирует агента СУМИ на сервере СУМИ.

Создание одноразового токена для идентификации агента:

```
$ bin/spire-server token generate -spiffeID spiffe://example.org/myagent

Token: <token_string>
```

Созданный токен необходимо записать, для идентификации агента при первоначальном запуске.

4.3. Запуск СУМИ агента

Агенты СУМИ запрашивают сервер СУМИ для аутентификации узлов и сервисов.

Для запуска и аутентификации агента необходим токен, созданный в пункте 3.2:

```
$ bin/spire-agent run -config conf/agent/agent.conf -joinToken
<token_string> &
```

```
...
INFO[0000] Starting workload API   subsystem_name=endpoints
```

Убедиться в работе агента:

```
$ bin/spire-agent healthcheck
Agent is healthy.
```

4.4. Создание политик регистрации для Сервиса

Чтобы СУМИ идентифицировал сервис, необходимо зарегистрировать сервис на СУМИ сервере с помощью регистрационных записей. Регистрация сервиса сообщает СУМИ, как идентифицировать сервис и какой СУМИ ID ей присваивать.

Создание регистрационной записи на основе UID текущего пользователя ($(id -u)):

```
$ bin/spire-server entry create -parentID spiffe://example.org/myagent \
    -spiffeID spiffe://example.org/myservice -selector unix:uid:$(id -u)
Entry ID      : ac5e2354-596a-4059-85f7-5b76e3bb53b3
SPIFFE ID     : spiffe://example.org/myservice
Parent ID     : spiffe://example.org/myagent
TTL           : 3600
Selector      : unix:uid:501
```

4.5. Получение и просмотр x509-SVID

Эта команда повторяет процесс, который потребовался бы сервису для получения x509-SVID от агента. x509-SVID можно использовать для аутентификации сервиса в другом сервисе. Чтобы получить и записать x509-SVID в /tmp/:

```
$ bin/spire-agent api fetch x509 -write /tmp/
Received 1 bundle after 254.780649ms
SPIFFE ID:            spiffe://example.org/myservice
SVID Valid After:     2019-10-25 19:07:49 +0000 UTC
SVID Valid Until:     2019-10-25 20:07:21 +0000 UTC
Intermediate #1 Valid After: 2019-10-25 19:07:11 +0000 UTC
Intermediate #1 Valid Until: 2019-10-25 20:07:21 +0000 UTC
CA #1 Valid After:    2018-05-13 19:33:47 +0000 UTC
CA #1 Valid Until:    2023-05-12 19:33:47 +0000 UTC
```

```
Writing SVID #0 to file /tmp/svid.0.pem.
Writing key #0 to file /tmp/svid.0.key.
Writing bundle #0 to file /tmp/bundle.0.pem.
```

Для просмотра содержимого SVID необходимо ввести команду openssl:

```
$ openssl x509 -in /tmp/svid.0.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            a2:76:ed:12:58:b0:1e:9f:9a:5b:42:60:b4:b1:52:b8
    Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=US, O=SPIFFE
        Validity
            Not Before: Oct 25 19:07:49 2019 GMT
            Not After : Oct 25 20:07:21 2019 GMT
        Subject: C=US, O=SPIRE
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:62:3d:4f:3d:21:d1:cc:c4:8b:89:c8:b2:a9:f0:
                    bd:88:89:3d:c3:a6:fe:25:27:18:6b:56:b2:2c:9c:
                    78:8c:40:cc:50:4d:e7:8a:8e:c0:c9:77:69:23:a6:
                    ca:b7:97:42:dc:12:1c:1d:c7:82:26:8a:4e:d9:59:
                    0f:1e:15:ac:e8
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
```

```
                Digital Signature, Key Encipherment, Key Agreement
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:

9D:B4:3C:3A:D7:9C:3A:3D:FE:9D:00:47:5A:22:06:3B:95:4B:6A:40
            X509v3 Authority Key Identifier:

keyid:21:12:95:72:50:9E:B1:E5:BA:35:78:65:49:62:3C:0B:5C:4C:07:BD
            X509v3 Subject Alternative Name:
                URI:spiffe://example.org/myservice
    Signature Algorithm: ecdsa-with-SHA384
         30:65:02:31:00:93:3c:f3:bd:cd:28:21:8f:dc:a9:bf:0b:41:
         34:21:54:cb:15:a0:92:9d:89:f8:f8:cc:49:e5:b7:e3:bd:0b:
         4f:a1:1a:46:ed:49:85:11:89:df:27:c1:06:72:7d:cd:bf:02:
         30:7b:ab:99:9e:bd:5d:ea:0d:05:85:f6:4e:18:11:8c:2d:f3:
         de:07:b5:e7:b7:6b:fe:b2:97:9c:41:d4:31:dd:7f:10:be:e4:
         75:ed:a4:bf:c3:ae:da:1d:28:4b:dc:2b:b5
```