Руководство пользователя
Программы для ЭВМ «Система управления межсервисной идентификацией»

На 17 листах

ООО «ЭйТи Консалтинг»

2023 г.

Содержание

1 Общие положения 4
1.1 Полное наименование Программы для ЭВМ, обозначение 4
1.2 Разработчик системы 4
1.3 Назначение документа 4
2 Настройка 5
2.1 Настройка доверенного домена 5
2.2 Настройка портов 6
2.3 Настройка аттестации узлов 6
2.4 Аттестация узлов под управлением Kubernetes 6
2.5 Токены сервисного аккаунта 7
2.6 Аттестация узлов под управлением Linux 7
2.7 Подключение токена 7
2.8 Сертификат X.509 8
2.9 Сертификат SSH 9
2.10 Настройка идентификации сервиса 9
2.11 Идентификация сервисов в Kubernetes 10
2.12 Идентификация сервисов для процессов Unix 10
2.13 Настройка места хранения данных агента и сервера 10
2.14 Настройка хранения данных сервера 11
2.15 Настройка SQLite 11
2.16 Настройка MySQL 12
2.1 Настройка Postgres 13
2.1 Настройка хранения сгенерированных ключей на Агенте и Сервере 13
2.2 Настройка доверительного корня 14
2.3 Настройка ключа подписи на диске 15
2.4 Настройка диспетчера секретов AWS 15
2.5 Настройка диспетчера сертификатов AWS 15
2.6 Экспорт метрик для мониторинга 16
2.1 Журнал логирования 17

Обозначения и сокращения

Обозначение / сокращение, термин	Расшифровка
ПО	Программное обеспечение
ЭВМ	Электронная вычислительная машина
СУМИ	Система управления межсервисной идентификацией

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 Настройка

СУМИ Сервер и агент настраиваются в файле с именами server.conf и agent.conf соответственно. По умолчанию Сервер ожидает, что файл конфигурации будет находиться в conf/server/server.conf, однако Сервер можно настроить на использование файла конфигурации в другом месте с помощью флага --config.

Точно так же Агент ожидает, что этот файл будет находиться в conf/agent/agent.conf, однако Сервер можно настроить на использование файла конфигурации в другом месте с помощью флага --config.

Файл конфигурации загружается один раз при запуске Сервера или Агента. Если файл конфигурации для любого из них изменен, сервер или агент необходимо перезапустить, чтобы конфигурация вступила в силу.

При запуске СУМИ в Kubernetes файл конфигурации обычно сохраняется в объекте ConfigMap, который затем монтируется как файл в контейнер, на котором запущен процесс агента или сервера.

2.1 Настройка доверенного домена

Доверенный домен соответствует доверенному корню поставщика удостоверений СУМИ. Доверенный домен может представлять человека, организацию, среду или отдел, использующие собственную независимую инфраструктуру СУМИ. Всем сервисам, идентифицированным в одном и том же доверенном домене, выдаются идентификационные документы, которые можно проверить по корневым ключам доверенного домена.

Каждый СУМИ сервер связан с одним доверенным доменом, который должен быть уникальным в пределах этой организации. Доверенный домен принимает ту же форму, что и DNS-имя, однако ему не обязательно соответствовать какой-либо инфраструктуре DNS.

Доверенный домен настраивается на СУМИ сервере перед его первым запуском. Он настраивается с помощью параметра trust_domain в разделе сервера в файле конфигурации. Например, если доверенный домен сервера должен быть настроен на prod.ru, тогда он будет установлен следующим образом:

```
trust_domain = "prod.ru"
```

Точно так же агент должен быть настроен для выдачи удостоверений в тот же доверенный домен путем настройки параметра trust_domain в разделе агента файла конфигурации агента.

СУМИ сервер и агент могут выдавать удостоверения только одному доверенному домену, и доверенный домен, настроенный агентом, должен совпадать с доверенным доменом сервера, к которому он подключается.

2.2 Настройка портов

По умолчанию СУМИ сервер прослушивает порт 8081 для входящих подключений от СУМИ агентов; чтобы выбрать другое значение, необходимо скорректировать параметр bind_port в файле server.conf. Например, чтобы изменить порт прослушивания на 9090:

```
bind_port = "9090"
```

Если эта конфигурация отличается от стандартной на сервере, то конфигурация обслуживающего порта также должна быть изменена на агентах.

2.3 Настройка аттестации узлов

СУМИ Сервер идентифицирует и аттестует агентов посредством процесса аттестации и разрешения узлов. Это достигается с помощью подключаемых модулей Node Attestor и Node Resolver, которые настраиваются и включаете на сервере.

Выбор метода аттестации узла определяет, какие подключаемые модули аттестатора узлов необходимо настроить для использования СУМИ в разделах подключаемых модулей сервера и подключаемых модулей агента файлов конфигурации СУМИ. Необходимо настроить по крайней мере один аттестатор узла на сервере и только один аттестатор узла на каждом агенте.

2.4 Аттестация узлов под управлением Kubernetes

Чтобы выдавать удостоверения сервисам, работающим в кластере Kubernetes, необходимо развернуть СУМИ агент на каждом узле в этом кластере, на котором работает сервис.

Токены сервисного аккаунта можно проверить с помощью Kubernetes Token Review API. Из-за этого СУМИ сервер не обязательно должен работать в Kubernetes, а один СУМИ сервер может поддерживать агенты, работающие в нескольких кластерах Kubernetes с включенной аттестацией PSAT.

Аттестация узла с использованием токенов прогнозируемой учетной записи службы (PSAT) Kubernetes позволяет СУМИ серверу проверять личность СУМИ агента, работающего в кластере Kubernetes. Токены прогнозируемой учетной записи службы обеспечивают дополнительные гарантии безопасности по сравнению с традиционными токенами учетной записи службы Kubernetes, и при поддержке кластера Kubernetes PSAT является рекомендуемой стратегией аттестации.

2.5 Токены сервисного аккаунта

В случаях, когда сервисы выполняются в Kubernetes, но функция прогнозируемого токена учетной записи службы недоступна для кластера, в котором они выполняются, СУМИ может установить доверительные отношения между сервером и агентом с помощью токенов учетной записи службы. В отличие от использования токенов спроецированной учетной записи службы, этот метод требует, чтобы СУМИ сервер и агент были развернуты в одном и том же кластере Kubernetes.

Поскольку токен учетной записи службы не содержит утверждений, которые можно было бы использовать для строгой идентификации узла/демонсета/модуля, на котором запущен агент, любой контейнер, запущенный в разрешенной учетной записи службы, может маскироваться под агента. По этой причине настоятельно рекомендуется, чтобы агенты запускались под выделенной учетной записью службы при использовании этого метода аттестации.

2.6 Аттестация узлов под управлением Linux

СУМИ может подтверждать подлинность сервисов, на которых выполняются физические или виртуальные машины (узлы) под управлением Linux. В рамках процесса аттестации СУМИ серверу необходимо установить доверие к СУМИ агенту, работающему на узле Linux. СУМИ поддерживает различные аттестаторы узлов в зависимости от того, где работает узел, что позволяет использовать разные селекторы при создании регистрационных записей для определения конкретных сервисов.

2.7 Подключение токена

Маркер присоединения — это простой метод аттестации сервера для агента с использованием одноразового маркера, который создается на сервере и передается агенту при запуске агента. Он работает на любом узле под управлением Linux.

СУМИ сервер можно настроить для поддержки аттестации токена присоединения, включив встроенный подключаемый модуль NodeAttestor для токена присоединения с помощью следующего раздела в файле конфигурации server.conf:

```
NodeAttestor "join_token" {

    plugin_data {

    }

}
```

После настройки аттестации узла токена присоединения на сервере можно сгенерировать токен присоединения с помощью команды spire-server token generate. При необходимости можно связать конкретный идентификатор СУМИ с токеном присоединения с помощью флага -spiffeID.

При первом запуске СУМИ агента с включенной аттестацией токена присоединения агент можно запустить с помощью команды запуска spire-agent и указать токен присоединения, сгенерированный сервером, с помощью флага -joinToken.

Сервер проверит токен присоединения и выдаст агенту SVID, и SVID будет автоматически чередоваться до тех пор, пока он поддерживает соединение с сервером. При последующих запусках агент будет использовать этот SVID для аутентификации на сервере, если только он не истек и не обновляется.

Чтобы использовать аттестацию узла токена присоединения, настройте и включите подключаемый модуль аттестатора узла токена присоединения на СУМИ сервере и СУМИ агенте.

Чтобы отключить аттестацию токена присоединения на сервере, закомментируйте или удалите этот раздел из файла конфигурации перед его запуском.

2.8 Сертификат X.509

Во многих случаях, особенно когда узлы инициализируются вручную (например, в центре обработки данных), узел может быть идентифицирован путем проверки существующего сертификата X.509, который ранее был установлен на узле, и однозначно идентифицирует его.

Обычно эти конечные сертификаты генерируются из одного общего ключа и сертификата (для целей данного руководства они будут называться пакетом корневых сертификатов). Сервер должен быть настроен с корневым ключом и любыми

промежуточными сертификатами, чтобы иметь возможность проверять конечный сертификат, представленный конкретной машиной. Только когда сертификат, который может быть проверен цепочкой сертификатов на сервере, будет найден, аттестация узла будет успешной, и рабочие нагрузки на этом узле смогут выдавать идентификаторы СУМИ.

Кроме того, attestor предоставляет селектор subject:cn, который будет соответствовать любому сертификату, который является одновременно действительным и чье общее имя соответствует описанному в селекторе.

Чтобы использовать аттестацию узла сертификата X.509, настройте и включите подключаемый модуль x509pop Node Attestor на СУМИ сервере и СУМИ агенте.

2.9 Сертификат SSH

В некоторых средах каждому узлу автоматически предоставляется действительный и уникальный сертификат SSH, который идентифицирует узел. СУМИ может использовать этот сертификат для начальной загрузки своей идентификации.

Узлам, аттестованным с помощью этого метода, автоматически присваивается СУМИ ID в виде:

```
spiffe://<trust-domain>/spire/agent/sshpop/<fingerprint>
```

Где <fingerprint> — это хэш самого сертификата. Затем этот идентификатор СУМИ можно использовать в качестве основы для других регистрационных записей сервисов.

Чтобы использовать аттестацию узла сертификата SSH, настройте и включите подключаемый модуль sshpop Node Attestor на СУМИ сервере и СУМИ агенте.

2.10 Настройка идентификации сервиса

В то время как аттестация узла касается того, как СУМИ сервер идентифицирует СУМИ агента на конкретной физической или виртуальной машине, идентификация сервисов касается того, как СУМИ агент идентифицирует конкретный процесс. Обычно они используются совместно для определения конкретных сервисов.

Как и в случае аттестации узла, идентификация сервисов выполняется путем включения соответствующих подключаемых модулей. Различные подключаемые модули предоставляют разные селекторы, которые можно использовать в регистрационных записях для определения конкретных сервисов. В отличие от аттестации узла, где для любого заданного сервиса одновременно может использоваться только одна стратегия,

идентификация сервисов может включать несколько стратегий для одного сервиса. Например, может потребоваться, чтобы один сервис выполнялся в определенной группе Unix и запускался из определенного образа Docker.

2.11 Идентификация сервисов в Kubernetes

Когда сервисы выполняются в контейнере Docker, может быть полезно иметь возможность описать их с точки зрения атрибутов этого контейнера, таких как образ Docker, из которого был запущен контейнер, или значение определенной переменной среды.

Плагин Docker Workload Attestor работает, опрашивая локальный демон Docker, чтобы получить специфичные для Docker метаданные о конкретном процессе, когда он вызывает Workload API.

2.12 Идентификация сервисов для процессов Unix

Когда сервисы выполняются в Unix, может быть полезно иметь возможность описать их с точки зрения того, как этот процесс управляется Unix, например, имя группы unix, в которой он выполняется.

Unix Workload Attestor работает, определяя метаданные ядра из сервисов, вызывающей Workload API, путем проверки вызывающей стороны сокета домена Unix.

2.13 Настройка места хранения данных агента и сервера

Параметр data_dir в файлах конфигурации agent.conf и server.conf задает каталог для данных времени выполнения СУМИ.

Если вы укажете относительный путь для data_dir, начав путь с ./, то data_dir оценивается на основе текущего рабочего каталога, из которого вы выполнили команду spire-agent или spire-server. Использование относительного пути для data_dir может быть полезно для первоначальной оценки СУМИ, но для производственных развертываний может потребоваться установить для data_dir абсолютный путь. По соглашению указать «/opt/spire/data» для data_dir, если СУМИ установлен в /opt/spire.

Необходимо убедится, что путь, указанный для data_dir, и все подкаталоги доступны для чтения пользователю Linux, который запускает исполняемый файл СУМИ агент или сервер. Можно использовать chown, чтобы изменить владельца этих каталогов данных на пользователя Linux, который будет запускать исполняемый файл.

Если путь, указанный для data_dir, не существует, исполняемый файл СУМИ агента или сервера создаст путь, если у пользователя Linux, который запускает исполняемый файл, есть соответствующие разрешения.

Обычно следует использовать значение для data_dir в качестве базового каталога для других путей к данным, которые настраиваются в файлах конфигурации agent.conf и server.conf. Например, если установлено для data_dir значение «/opt/spire/data» в файле agent.conf, необходимо установить для KeyManager «disk» каталог plugin_data значение «/opt/spire/data/agent». Или, если установлено для data_dir значение /opt/spire/data в server.conf, необходимо установить для connection_string значение «/opt/spire/data/server/datastore.sqlite3», если используется SQLite для хранилища данных СУМИ сервера.

2.14 Настройка хранения данных сервера

Хранилище данных — это место, где сервер СУМИ сохраняет динамическую конфигурацию, такую как записи регистрации и политики сопоставления удостоверений, которые извлекаются с СУМИ сервера. По умолчанию СУМИ связывает SQLite и устанавливает его по умолчанию для хранения данных сервера. СУМИ также поддерживает другие совместимые хранилища данных.

СУМИ Сервер можно настроить для использования различных SQL-совместимых серверных хранилищ данных, настроив подключаемый модуль хранилища данных SQL по умолчанию.

2.15 Настройка SQLite

По умолчанию СУМИ сервер создает и использует локальную базу данных SQLite для резервного копирования и хранения данных конфигурации. Хотя это удобно для тестирования, обычно не рекомендуется для производственных развертываний, поскольку сложно совместно использовать хранилище данных SQLite на нескольких машинах, что может усложнить резервное копирование, развертывание высокой доступности и обновления.

Чтобы настроить сервер для использования базы данных SQLite, необходимо включить раздел в файле конфигурации, который выглядит следующим образом:

```
DataStore "sql" {

        plugin_data {
```

```
            database_type = "sqlite3"

            connection_string = "/opt/spire/data/server/datastore.sqlite3"

        }

    }
```

В файле конфигурации не должно быть других (не закомментированных) разделов DataStore.

База данных будет создана по пути, указанному в connection_string.

2.16 Настройка MySQL

В производственной среде рекомендуется использовать выделенную базу данных для резервного копирования и хранения данных конфигурации.

Пользователь MySQL, который имеет возможность подключаться к любому экземпляру EC2, на котором работает СУМИ сервер, и который может редактировать базу данных.

Чтобы настроить СУМИ сервер для использования базы данных MySQL, включите раздел в файле конфигурации, который выглядит следующим образом:

```
DataStore "sql" {

        plugin_data {

            database_type = "mysql"

            connection_string =
"username:password@tcp(localhost:3306)/dbname?parseTime=true"

        }

    }
```

В приведенной выше строке подключения необходимо заменить следующее:

- Username - имя пользователя MySQL, которое должно использоваться для доступа к базе данных
- Password - пароль пользователя MySQL
- localhost:3306 - IP-адрес или имя хоста сервера MySQL и номер порта
- dbname - имя базы данных

2.1 Настройка Postgres

В производственной среде рекомендуется использовать данную базу данных для резервного копирования и хранения данных конфигурации. Для сервера СУМИ требуется:

- Выделенная база данных на сервере Postgres для настройки СУМИ сервера
- Пользователь Postgres, который имеет возможность подключаться к любому экземпляру, на котором работает СУМИ сервер, и который может редактировать базу данных.

Чтобы настроить СУМИ сервер для использования базы данных Postgres, включите следующий раздел в файле конфигурации сервера:

```
DataStore "sql" {

        plugin_data {

            database_type = "postgres"

            connection_string = "dbname=[database_name] user=[username]

                                password=[password] host=[hostname]
port=[port]"

        }

    }
```

Значение connection_string имеет формат ключ = значение, однако также можно использовать URI подключения.

В приведенной выше строке подключения необходимо заменить следующее:

- [database-name] - имя базы данных
- [username] - имя пользователя Postgres, обращающегося к базе данных
- [password] - пароль пользователя
- [hostname] - IP-адрес или имя хоста сервера Postgres
- [port] - номер порта сервера Postgres

2.1 Настройка хранения сгенерированных ключей на Агенте и Сервере

Как СУМИ агент, так и СУМИ сервер генерируют закрытые ключи и сертификаты во время нормальной работы. Важно поддерживать целостность этих ключей и сертификатов, чтобы обеспечить целостность выданных идентификаторов СУМИ.

В настоящее время СУМИ поддерживает две стратегии управления ключами как на агенте, так и на сервере.

Хранить в памяти. В этой стратегии ключи и сертификаты хранятся только в памяти. Это означает, что в случае сбоя или перезапуска сервера или агента ключи необходимо сгенерировать заново. В случае с СУМИ агентом обычно требуется повторная аттестация агента на сервере после перезапуска. Этой стратегией можно управлять, включив и настроив подключаемый модуль диспетчера ключей памяти для СУМИ сервера и/или СУМИ агента.

Хранить на диске. В этой стратегии ключи и сертификаты хранятся в указанном файле на диске. Преимущество этого подхода в том, что они выдерживают перезапуск СУМИ сервера или СУМИ агента. Недостатком является то, что, поскольку ключи хранятся в файлах на диске, необходимо принять дополнительные меры предосторожности, чтобы предотвратить чтение этих файлов вредоносным процессом. Этой стратегией можно управлять, включив и настроив подключаемый модуль диспетчера дисковых ключей для СУМИ сервера и/или СУМИ агента.

Кроме того, СУМИ можно настроить для интеграции пользовательского бэкэнда, такого как хранилище секретов, с помощью сторонних подключаемых модулей диспетчера ключей.

2.2 Настройка доверительного корня

Каждый СУМИ сервер использует определенный корневой ключ подписи, который используется для выполнения нескольких важных действий:

- Чтобы установить доверие СУМИ агента к СУМИ серверу, поскольку агент имеет сертификат, подписанный этим ключом (доверие между сервером и агентом устанавливается посредством идентификации).
- Для создания X.509 или JWT SVID, выдаваемых сервисам
- Для создания доверительных пакетов СУМИ (используемых для установления доверительных отношений с другими СУМИ серверами)

Этот ключ подписи следует считать крайне конфиденциальным, так как его получение позволит злоумышленнику выдать себя за СУМИ сервер и выдавать удостоверения от его имени.

Чтобы обеспечить целостность ключа подписи, СУМИ сервер может либо сам подписывать материал с помощью ключа подписи, хранящегося на диске, либо

делегировать подписание независимому центру сертификации, например AWS Secrets Manager. Это поведение настраивается через раздел UpstreamAuthority в файле server.conf.

2.3 Настройка ключа подписи на диске

СУМИ сервер можно настроить на загрузку учетных данных центра сертификации с диска, используя их для создания промежуточных сертификатов подписи для центра подписи сервера.

СУМИ сервер поставляется с «фиктивным» ключом и сертификатом, которые можно использовать для упрощения тестирования, однако, поскольку этот же ключ распространяется среди всех пользователей СУМИ, его нельзя использовать ни для чего, кроме целей тестирования. Вместо этого следует сгенерировать ключ подписи на диске.

Если инструмент openssl установлен, действительный корневой ключ и сертификат можно сгенерировать с помощью команды, подобной следующей:

```
sudo openssl req \
       -subj "/C=/ST=/L=/O=/CN=acme.com" \
       -newkey rsa:2048 -nodes -keyout /opt/spire/conf/root.key \
       -x509 -days 365 -out /opt/spire/conf/root.crt
```

Этой стратегией можно управлять, включив и настроив подключаемый модуль диска UpstreamAuthority для СУМИ сервера.

2.4 Настройка диспетчера секретов AWS

СУМИ сервер можно настроить на загрузку учетных данных центра сертификации из Amazon Web Services Secrets Manager, используя их для создания промежуточных сертификатов подписи для центра подписи сервера.

Этой стратегией можно управлять, включив и настроив плагин awssecret UpstreamAuthority для СУМИ сервера.

2.5 Настройка диспетчера сертификатов AWS

СУМИ сервер можно настроить на загрузку учетных данных из частного центра сертификации Amazon Web Services Certificate Manager для создания промежуточных сертификатов подписи для центра подписи сервера.

Этой стратегией можно управлять, включив и настроив подключаемый модуль aws_pca UpstreamAuthority для СУМИ сервера.

2.6 Экспорт метрик для мониторинга

Чтобы настроить СУМИ сервер или СУМИ агент для вывода данных в сборщик метрик, отредактируйте раздел телеметрии в server.conf или agent.conf. СУМИ может экспортировать метрики в Datadog (формат DogStatsD), M3, Prometheus и StatsD.

Можно настроить несколько коллекторов одновременно. DogStatsD, M3 и StatsD поддерживают несколько объявлений в случае, если необходимо отправить метрики более чем одному сборщику.

Ниже приведен пример блока конфигурации для agent.conf или server.conf, который экспортирует телеметрию в Datadog, M3, Prometheus и StatsD и отключает сборщик в памяти:

```
telemetry {
        Prometheus {
                port = 9988
        }

        DogStatsd = [
            { address = "localhost:8125" },
        ]

        Statsd = [
            { address = "localhost:1337" },
            { address = "collector.example.org:8125" },
        ]

        M3 = [
            { address = "localhost:9000" env = "prod" },
        ]

        InMem {
```

```
            enabled = false

        }

}
```

2.1 Журнал логирования

Расположение файла журнала и уровень ведения журнала для СУМИ сервера и СУМИ агента можно указать в соответствующих файлах конфигурации. Необходимо отредактировать значение log_file, чтобы задать расположение файла журнала, и значение log_level, чтобы задать уровень ведения журнала. Это может быть DEBUG, INFO, WARN или ERROR.

По умолчанию журналы СУМИ помещаются в STDOUT. Однако вместо этого СУМИ агент и СУМИ сервер можно настроить для записи журналов непосредственно в файл, указав путь к файлу в атрибуте log_file.