AT Consulting

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая
Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

ЦУП Модуль управления секретами

Краткий обзор основных функциональных возможностей.

Оглавление:

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Архитектурные решения

1. Множественное подключение (Кластеризация на уровне БД)

Указание начиная с какой версии: с 12-го релиза

Краткое описание:

Был разработан storage backend в соответствии со спецификациями интерфейсов physical.go, далее - patroni storage backend, поддерживающий в качестве СУБД один или более кластеров PostgreSQL на базе Patroni с настроенной между кластерами асинхронной физической репликацией. Patroni storage backend предоставляет набор метрик/телеметрии оригинального postgresql storage backend. Реализация patroni storage backend позволяет использовать его в качестве storage backend в Vault.

Поддерживаемые конфигурации:

1. Один кластер PostgreSQL :

   a. кластер, включающий два узла PostgreSQL и арбитр, между узлами PostgreSQL кластера настроена синхронная физическая репликация.

2. Два кластера PostgreSQL:

   a. Мастер-кластер, включающий два узла PostgreSQL и арбитр, между узлами PostgreSQL кластера настроена синхронная физическая репликация.

StandBy кластер, включающий два узла PostgreSQL и арбитр, между узлами PostgreSQL кластера настроена синхронная физическая репликация, между кластерами настроена асинхронная физическая репликация.

Описание настройки:

Параметры настройки patroni storage backend:

storage "patroni" {

connection_urls = ["postgres://user:pass12@12.13.14.15:6432,12.13.14.15:8432,12.13.14.15:9432/vault1?sslmode=disable&statement_cache_mode=describe", "postgres://anna12:anna12@112.113.114.115:6432,112.113.114.115:8432/vault1?sslmode=disable&statement_cache_mode=describe"]

wait_for_answer_timeout = 0.1

max_write_wait_timeout = 13

ha_enabled = "true"

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
        max_parallel = 350
}
ha_storage "patroni" {
        connection_urls =
        ["postgres://user:pass12@12.13.14.15:4657,12.13.14.15:3654,12.13.14.15:6589/vault_ha?
        sslmode=disable&statement_cache_mode=describe",
        "postgres://anna12:anna12@112.113.114.115:6432,112.113.114.115:8432/vault_ha?sslmo
        de=disable&statement_cache_mode=describe"]
        wait_for_answer_timeout = 0.1
        max_write_wait_timeout = 13
        max_parallel = 350
}
```

Способ проверки:

Шаг 1. Отключаем сервер БД на slave.

Vault сохраняет работоспособность.

Шаг 2. Включить обратно сервер БД Slave.

Шаг 3. Отключаем сервер БД на master

Запустился процесс смены мастера Vault.

Vault сохраняет работоспособность.

Шаг 4. Включить обратно сервер БД Master.

Шаг 5. Переключаем мастера БД.

Запустился процесс смены мастера Vault.

Vault сохраняет работоспособность.

2. Чтение со standby узлов (Кластеризация на уровне vault)

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Указание начиная с какой версии: с 16-го релиза.

Краткое описание:

Доработка заключается в обеспечении горизонтального масштабирования производительности системы для запросов, которые не приводят к записи информации в базу данных (физический бэкенд). Масштабирование должно обеспечиваться путем обработки таких запросов на stand-by узлах, с перенаправлением «неподходящих» запросов на лидера кластера.

Таким образом, для решения поставленной задачи необходимо реализовать следующие функции:

1. Фильтрация запросов на stand-by узлах и перенаправление на лидера тех запросов, которые не могут быть обработаны на stand-by узлах.
2. Авторизация запросов на стороне stand-by узлов.
3. Актуализация кэша stand-by узлов, при изменении кэша лидера.

Описание настройки:
Формирование списка активных stand-by узлов:

Список узлов и статус их активности формируется путем передачи heartbeat-запросов от stand-by узлов к лидеру, с использованием текущего механизма.

Heartbeat-запрос содержит следующие поля:

1. hostname – например "node1",
2. api_address – например "http://10.0.0.2:8200",
3. cluster_address – например "https://10.0.0.2:8201",
4. active_node – true, если готов обрабатывать запросы (статус Running или Unsealing), иначе false
5. last_echo – например "2021-11-29T10:29:09.202235-05:00"

При получении heartbeat-запроса, лидер кластера запоминает присланные данные для последующего использования.

Узел считается активным, если поле active_node равняется “true”, а время от предыдущего heartbeat-запроса до текущего времени не превышает максимальный период между heartbeat.

Шаги проверки:

Шаг 1. В конфигурационном файле Vault включаем обработку на standby узлах.

Шаг 2. Запрашиваем статус кластера “/sys/ha-status”.

Шаг 3. Подаем нагрузку в Vault посредством JMeter запросы на чтение. Фиксируем значение производительности в JMeter.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Шаг 4. Подаем нагрузку в Vault посредством JMeter запросы на запись. Фиксируем значение производительности в JMeter.

Шаг 5. В конфигурационных файлах Vault включаем чтение на standby узлах (2 standby ноды).

Шаг 6. Запрашиваем статус кластера “/sys/ha-status” .

Шаг 7. Подаем нагрузку в Vault посредством JMeter запросы на чтение. Фиксируем значение производительности в JMeter.

Шаг 8. Подаем нагрузку в Vault посредством JMeter запросы на запись. Фиксируем значение производительности в JMeter.

3. Stand In (Холодное резервирование)

Указание начиная с какой версии: с 12-го релиза

Краткое описание:

Stand in (Холодное резервирование) – полнофункциональный набор компонентов, обладающий в любой момент времени актуальной копией данных.

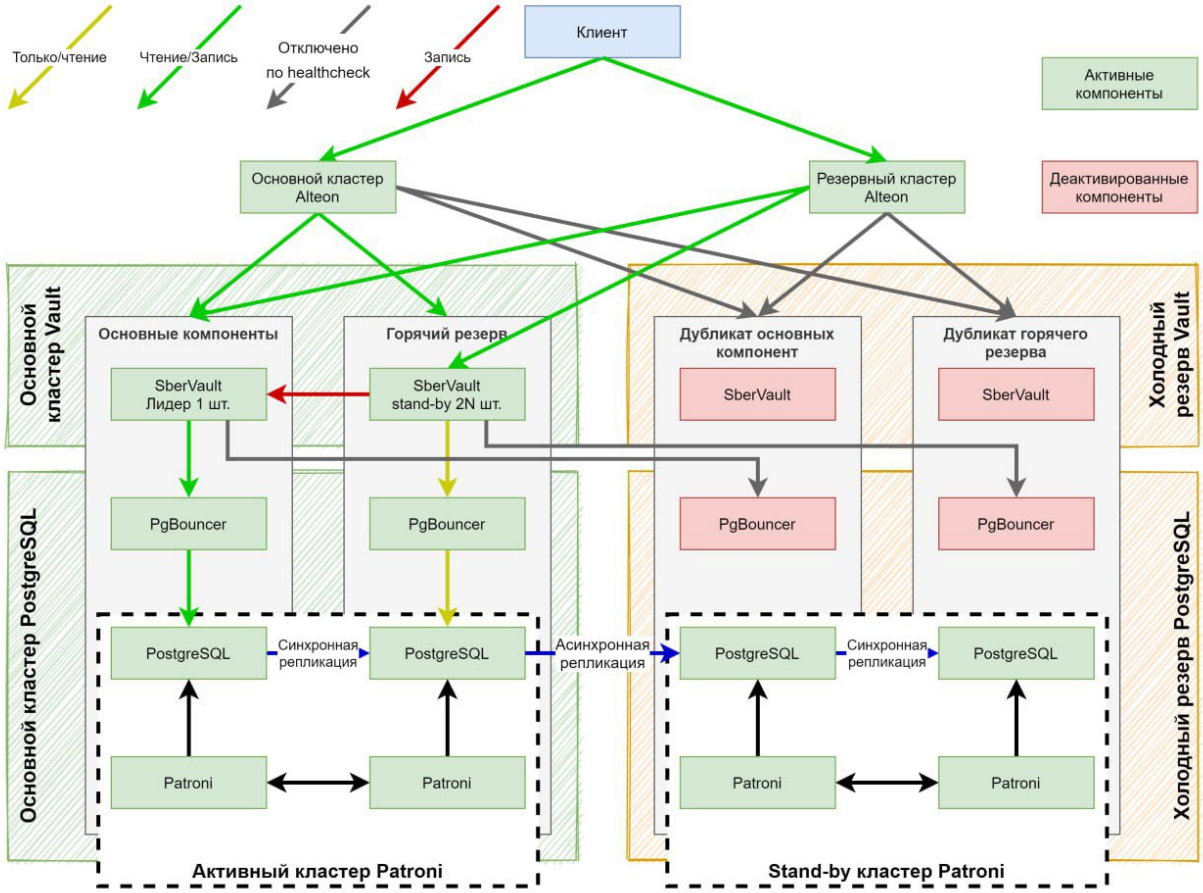
Stand in осуществляет резервирование не только функциональных компонентов, но и компонентов, которые реализуют нефункциональные требования по обеспечению горячего резерва.

Таким образом при переключении на холодный резерв, система будет защищена от сбоев дубликатом горячего резерва. Холодный резерв сможет функционировать в качестве основных мощностей, а те мощности, которые были выведены из строя, после восстановления должны стать холодным резервом. Компоненты холодного резерва должны быть деактивированы, за исключением серверов PostgreSQL. Балансировщик должен быть настроен на серверы холодного резерва, чтобы при активации кластера начать подавать на него трафик. Для обеспечения актуальности копии данных, серверы PostgreSQL должны быть активны и настроены на каскадную репликацию с серверов основного кластера.

Полная схема холодного резерва:

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru



Функциональные возможности

1. Двухфакторная аутентификация (2FA)

Указание начиная с какой версии: с 13-го релиза

Краткое описание:

Двухфакторная аутентификация (2fa) реализована с использованием модифицированного движка аутентификации ldap_2fa и интеграции с провайдером одноразовых паролей LinOTP (https://linotp.org/).

При аутентификации движок получает от пользователя не только логин и пароль, но и одноразовый код otp в случае, если в каталоге ldap данный пользователь состоит в группе обязывающей его использовать (группа 2fa, см параметр 2fa_group_name).

Описание настройки:

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

1. Настроить движок аутентификации для подключения к LinOTP

```
{
  // адрес AD
  "url": "ldap://10.53.219.186:389",
  "linotp_url": [
     // адрес сервера LinOTP
     "https://10.56.100.168",
  ],
  "linotp_realm": "delta_devi",
  "2fa_group_name": "force_mfa_group",
  “linotp_certificate” : “указывается сертификат, если сертификат сервера не является доверенным с точки зрения операционной системы”,
  "linotp_insecure_tls": false,
  "binddn": "cn=linotp,cn=users,dc=dev_ad,dc=test,dc=vault",
  "upndomain": "dev_ad.test.vault",
  "case_sensitive_names": true,
  "groupdn": "cn=Users,dc=dev_ad,dc=test,dc=vault",
  "userdn": "cn=Users,dc=dev_ad,dc=test,dc=vault",
  "bindpass": "Mypassword123",
  "groupattr": "cn",
  "insecure_tls": false,
  "starttls": true,
    "groupfilter": "(|(memberUid={{.Username}})(member={{.UserDN}})(uniqueMember={{.UserDN}}))"
}
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Шаги проверки:

Предусловие, настроен движок аутентификации ldap, создан пользователь в каталоге ldap и он же добавлен в группу AD, требующую проверки otp пароля (группа 2fa, см параметр 2fa_group_name). Для пользователя привязан генератор паролей на портале самообслуживания, например, https://10.56.100.168/selfservice/login. Где 10.56.100.168 - IP адрес LinOTP. С помощью устройства вывода, обеспечено получение актуального OTP пароля.

1. В UI демонстрируется способы аутентификации на сервере Vault, включаю форму ldap_2fa.
2. В UI выполняется аутентификация с указанием логина пользователя, пароля пользователя и OTP пароля.
    a. Аутентификация выполнена
3. В UI выполняется аутентификация с указанием логина пользователя, пароля пользователя из пункта 2.
    a. Аутентификация не выполнена. Для пользователя обязательна проверка OTP пароля

2. Выпуск сертификатов с использованием движка PKI

Указание начиная с какой версии: *с 1-го релиза*
(https://developer.hashicorp.com/vault/docs/secrets/pki)

Краткое описание:

Механизм секретов PKI Vault может динамически генерировать сертификаты X.509 по требованию. Это позволяет службам получать сертификаты, не проходя обычный ручной процесс генерации закрытого ключа и запроса на подписание сертификата (CSR), отправки в центр сертификации (ЦС), а затем ожидания завершения процесса проверки и подписания. Встроенные в Vault механизмы аутентификации и авторизации обеспечивают функциональность проверки. За счет относительно короткого TTL снижается вероятность необходимости отзыва сертификатов, что позволяет поддерживать короткие CRL и помогает механизму секретов масштабироваться для больших рабочих нагрузок. Это, в свою очередь, позволяет каждому экземпляру работающего приложения иметь уникальный сертификат, устраняя совместное использование и сопутствующие проблемы с отзывом и переносом сертификата. Кроме того, позволяя в основном отказаться от отзыва, этот механизм секретов позволяет использовать эфемерные сертификаты. Сертификаты могут быть извлечены и сохранены в памяти при запуске приложения и удалены при завершении работы без записи на диск.

Описание настройки:

Большинство механизмов секретов должны быть настроены заранее, прежде чем они

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

смогут выполнять свои функции. Эти шаги обычно выполняются оператором или инструментом управления конфигурацией.

1. Включить механизм секретов PKI:

$ vault secrets enable pki

По умолчанию движок секретов монтируется по имени движка. Чтобы включить механизм секретов по другому пути, нужно использовать аргумент -path.

2. Увеличить TTL, настроив движок секретов. Значение по умолчанию 30 дней может быть слишком коротким, поэтому можно увеличить его до 1 года:

$ vault secrets tune -max-lease-ttl=8760h pki

3. Настройка сертификата CA и закрытого ключа. Vault может принимать существующую пару ключей или создавать собственный самоподписанный корневой сертификат. Рекомендуется поддерживать корневой CA вне Vault и предоставлять Vault подписанный промежуточный CA.

```
$ vault write pki/root/generate/internal \
common_name=my-website.com \
ttl=8760h
```

TTL может быть указан в часах (h), минутах (m), секундах (s).

4. Обновить расположение CRL и выдачу сертификатов. Эти значения могут быть обновлены в будущем.

```
$ vault write pki/config/urls \
issuing_certificates="http://127.0.0.1:8200/v1/pki/ca" \
crl_distribution_points="http://127.0.0.1:8200/v1/pki/crl"
```

5. Настройка роли, которая сопоставляет имя в Vault с процедурой генерации сертификата. Когда пользователи или машины генерируют учетные данные, они генерируются на основе этой роли:

```
$ vault write pki/roles/2022-servers \
allowed_domains=my-website.com \
allow_subdomains=true \
max_ttl=72h
```

Шаги проверки:

Шаг 1. Создать корневой CA example.com,необходимо дать ему имя эмитента и

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

сохранить его сертификат в файле root_2022_ca.crt.:

```
$   vault write -field=certificate pki/root/generate/internal \
        common_name="example.com" \
        issuer_name="root-2022" \
        ttl=87600h > root_2022_ca.crt
```

Шаг 2. Настройка URL-адреса CA и CRL:

```
$   vault write pki/config/urls \
    issuing_certificates="$VAULT_ADDR/v1/pki/ca" \
    crl_distribution_points="$VAULT_ADDR/v1/pki/crl"
```

Шаг 3. Выполнить следующую команду для создания промежуточного сертификата и сохранитмь CSR как pki_intermediate.csr.

```
$   vault write -format=json pki_int/intermediate/generate/internal \
    common_name="example.com Intermediate Authority" \
    issuer_name="example-dot-com-intermediate" \
    | jq -r '.data.csr' > pki_intermediate.csr
```

3. Движок секретов Active Directory

Указание начиная с какой версии: *с 1-го релиза + доработан в* 13-м релизе

Краткое описание:

Движок секретов Active Directory Secret Engine (далее AD) способен:

с 1-го релиза (см. AD):

1. Поддерживать взаимодействие с контроллерами доменов версий:
    a. Windows Server 2012
    b. Windows Server 2016
    c. Windows Server 2019
2. Выполнять аутентификацию при взаимодействии с доменами Microsoft Active Directory по протоколам:
    a. Ldap
3. Выполнять операции : создания секретов, ротации секретов, удаления секретов.

Доработанная версия способна, в дополнении к коробочной версии:

1. Выполнять аутентификацию при взаимодействии с доменами Microsoft Active Directory по протоколам:
    a. Kerberos

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

2. Автоматически определять активные узлы кластера, доступные для выполнения требуемых операций, в том числе создания секретов, ротации секретов, удаления секретов.

Описание настройки:

Предусловие, движок AD активирован, установлено доверие между операционной системой и сервером ldap)

```
{
   "krb5conf": {
      "libdefaults": {

         "rdns": false

      },

      "realms": {

         "DEV_AD.TEST.VAULT": {

            "kdc": "tksss-pam000001.dev_ad.test.vault:88",

            "admin_server": "tksss-pam000001.dev_ad.test.vault"

         }

      },

      "domain_realm": {

         ".dev_ad.test.vault": "DEV_AD.TEST.VAULT",

         "dev_ad.test.vault": "DEV_AD.TEST.VAULT"

      }

   },

   "url": "ldaps://dev_ad.test.vault",

   "userdn": "cn=Users,dc=dev_ad,dc=test,dc=vault",

   "binddn": "Логин от  УЗ, с достаточными правами, для выполнения всех интеграционных взаимодействий ",

   "bindpass": "Пароль от binddn ",

   "realm": "DEV_AD.TEST.VAULT",

   "auth_mode": "krb_password",

   "ttl": 240,
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
"max_ttl": "2h",
"secret_validation_period": 0,
"insecure_tls": false,
"starttls": true,
"disable_pafxfast": true,
"assume_pre_authentication": false
```

Шаги проверки:

Шаг 1: Активировать движок

```
curl --request POST \
  --url https://.... /v1/sys/mounts/имя_движка \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "type":"ad"
}'
```

Шаг 2: Настроить движок

```
curl --request POST \
  --url https://.... /v1/имя_движка/config \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    См Описание настройки:
}'
```

Шаг 3: Создать статическую роль

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
curl --request POST \
  --url https://.... /v1/имя_движка/roles/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
   "service_account_name":"Имя ТУЗ, которую необходимо взять под управление"
   "ttl":"300"
}'
```

Шаг 4: Создать конфиг генерации кейтаб для статической роли

```
curl --request POST \
  --url https://.... /v1/имя_движка/roles/имя_роли/keytab \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
   "principal_name":"UPN ТУЗ, для которой ранее была создана статическая роль. См атрибут userPrincipalName в оснастке ADUC"
   "encryption":" AES256-CTS-HMAC-SHA1-96"
}'
```

Шаг 5: Получить пароль статической роли

```
curl --request GET \
  --url https://.... /v1/имя_движка/creds/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
}'
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523
Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Будет выдан на запрос пароль

Шаг 6: Получить кейтаб статической роли

```
curl --request GET \
  --url https://.... /v1/имя_движка/keytab/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
}'
```

Будет выдан на запрос кейтаб

Эксплуатационные решения

1. Журналирование (Системное логирование, Аудит движки (локальный аудит), выгрузка в сторонние системы)

Указание начиная с какой версии: *с 1-го релиза*

Краткое описание:

https://developer.hashicorp.com/vault/docs/audit

Vault имеет два типа журналов - журналы работы сервера Vault и журналы аудита. Журналы аудита записываются каждый запрос, сделанный в Vault, а также ответ, отправленный из Vault. Журналы сервера - это операционные журналы, которые дают представление о том, что сервер делает внутри и в фоновом режиме во время работы Vault.

Устройства аудита - это компоненты Vault, которые ведут подробный журнал всех запросов и ответов к Vault. Поскольку каждая операция с Vault - это запрос/ответ API, при использовании одного устройства аудита журнал аудита содержит все аутентифицированные взаимодействия с Vault, включая ошибки.

Каждая строка в журнале аудита представляет собой объект JSON. Поле type определяет тип объекта. В настоящее время существует только два типа: запрос и ответ. Строка содержит всю информацию для любого данного запроса и ответа. По умолчанию вся конфиденциальная информация сначала хэшируется перед записью в журнал аудита.

Доработки журналирования Vault Agent,13 релиз:

Vault agent, вне зависимости от среды исполнения, в том числе при работе в среде контейнерной оркестрации выполняет логгирование с возможностью отправки во внешние системы логгирования.Vault agent включает настройки, позволяющие выполнять

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

журналирование в файлы. Настройки позволяют указать несколько назначений для сохранения событий.Vault agent включает настройки ротации файлов журналов. Vault agent пишет логи в формате Standard, Json, LOGE в файл, так же пишет логи в консоль. В атрибутике логов добавлены параметры для точного определения проблемы события.

Описание настройки:

- *Локальный аудит:*
  1. Включить по пути по умолчанию:
  vault audit enable file file_path=/var/log/vault_audit.log
  Можно включить несколько копий устройства аудита
  2. Конфигурация для аудит движков (подача параметров конфигурации через пары K=V:):
  - file_path (string: <необходимо>) - Путь к месту записи журнала аудита. Если по указанному пути уже существует файл, бэкенд аудита будет добавлять его. Есть несколько специальных ключевых слов:
  - stdout - записывает журнал аудита в стандартный вывод
  - discard - записывает выходные данные (полезно в сценариях тестирования)
  - log_raw (bool: false) - Если включено, регистрирует конфиденциальную информацию безопасности без хеширования в сыром формате.
  - hmac_accessor (bool: true)- Если включено, включает хеширование доступа к токенам.
  - mode (string: "0600") - Строка, содержащая восьмеричное число, представляющее битовый шаблон для режима файла, аналогично chmod. Установите значение "0000", чтобы запретить Vault изменять режим файла.
  - format (string: "json") - Позволяет выбрать формат вывода. Допустимыми значениями являются "json" и "jsonx", которые форматируют обычные записи журнала в формате XML.
  - prefix (string: "") - Настраиваемый строковый префикс для записи перед фактической строкой журнала.

- *Системное логирование:*
  1. Устройство аудита syslog можно включить следующей командой:
  vault audit enable syslog2
  Подача параметров конфигурации через пары K=V:
  vault audit enable syslog tag="vault" facility="AUTH"
  2. Конфигурация для системного аудита :
  - facility (строка: "AUTH") - Используемый объект syslog.
  - tag (строка: "vault") - Используемый тег syslog.
  - log_raw (bool: false) - Если включено, информация, чувствительная к безопасности, записывается в журнал без хэширования, в необработанном формате.
  - hmac_accessor (bool: true) - Если включено, включает хэширование токена accessor.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

- mode (string: "0600") - Строка, содержащая восьмеричное число, представляющее битовый шаблон для режима файла, аналогично chmod.
- format (string: "json") - Позволяет выбрать формат вывода. Допустимыми значениями являются "json" и "jsonx", которые форматируют обычные записи журнала как XML.
- prefix (string: "") - настраиваемый строковый префикс для записи перед фактической строкой журнала.

- *Пример конфигурации журналирования в файл (выгрузка в сторонние системы):*

Для указания настроек логирования необходимо использовать stanza

```
log_destination
log_destination "Standard" {
log_format = "Standard"
log_path = "/var/log/vault"
log_file = "agent.log"
log_rotate = "1h"
log_max_size = "50m"
}
log_destination "Json" {
log_format = "Json"
log_path = "/var/log/vault"
log_file = "agent-pv.log"
log_level = "info"
}
```

Шаги проверки:

Шаг 1. Посмотреть список включенный устройств аудита

```
curl \
  --header "X-Vault-Token: ..." \
  http://127.0.0.1:8200/v1/sys/audit
```

2. Мониторинг

Указание начиная с какой версии: *с 1-го релиза*

Краткое описание:

https://developer.hashicorp.com/vault/tutorials/monitoring/monitor-telemetry-audit-splunk

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Система может отправлять подробные метрики операционной телеметрии в систему сбора метрик для мониторинга производительности системы, оповещения о превышении допустимых показателей нагрузки, а также для регистрации входящих и исходящих запросов. Присутствуют следующие функциональности:

- фильтр для отгружаемых системой метрик.
- выгрузка метрик по каждому тенанту. Метрики должны отражают нагрузку получения секретов по каждому тенанту.
- Для сокращения количества метрик данные показатели передаются агрегировано, с разделением по тенантам путем указания метки для метрики.
- отправка уведомлений при превышении пороговых значений контрольными параметрами Системы

Описание настройки:

Настройка производится через дашборды (на примере Dynatrace).

Необходимо настроить dashboard со следующими метриками (по умолчанию):

- CPU used %
- Memory used %
- File description max, used
- Disk used %
- barrier.get
- cache.hit.count
- postgres.get/vault.postgres.get (в зависимости от используемой версии БД)
- secret.lease.creation.count
- core.active

Пример критичности и пороговых значений для срабатывания уведомлений

Наименование	Критичность и пороговое значение для срабатывания						
File descriptors max, used	68.70 count	72.32 count	76.13 count	80.14 count	84.36 count	88.80 count	93.48 count
Disk used %	70%	75%	80,00%	85%	90%	95%	100%
Cpu usage %	70%	75%	80,00%	85%	90%	95%	100%
Memory used %	70%	75%	80,00%	85%	90%	95%	100%

Пример конфигурирования:

```
telemetry {
 disable_hostname = true
 enable_hostname_label = false
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
 statsd_address = "127.0.0.1:18125"
 prefix_filter = ["-vault.rollback", "-vault.route", "-vault.expire", "-vault.database", "-vault.secrets",
"+vault.expire.lease_expiration", "+vault.expire.num_leases", "+vault.token.count",
"+vault.secrets.kv.count"]
}
```

Разработанная функциональность

1. Тенанты (Namespaces)

Указание начиная с какой версии: *с 10-го релиза*

Краткое описание:

Шаблон пространства имен дает возможность реализовать безопасную многопользовательскую среду в Vault, чтобы обеспечить максимальную изоляцию секретов, гарантировать отдельным группам самостоятельно управлять своими собственными средами и предоставляет гибкую систему разграничения доступа на основе ролевой модели. Предполагается использовать подход с мультитенантностью, что позволит максимально изолировать секреты клиентов, упростит масштабирование и расширение.

- Тенант - изолированная область хранения секретов в Системе, доступ к которой определяется наличием пользователя в группе доступа.
- Для реализации работы с API и CLI доступны заголовки запросов - X-Vault-Namespace и -namespace соответственно.

Описание настройки:

Все методы работы с тенантами и namespaces предполагают выполнение с токенами, полученными в шагах проверки 5 и 6 соответственно.

Шаги проверки:

Шаг 1: Создать тенант

```
curl --request POST \
  --url https://.... /v1/sys/namespaces/имя_тенанта \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
  --data '{

}'
```

Шаг 2: Создать namespace

```
curl --request POST \

  --url https://.... /v1/имя_тенанта/sys/namespaces/имя_namespace \

  --header 'Content-Type: application/json' \

  --header 'X-Vault-Token: …' \

  --data '{

}'
```

Шаг 3: Создать парольную политику для тенанта

```
curl --request POST \

  --url https://.... /v1/sys/policy/имя__политики_тенанта \

  --header 'Content-Type: application/json' \

  --header 'X-Vault-Token: …' \

  --data '{

    "policy": "path \"sys/namespaces/api-lock/lock/+\" {capabilities = [\"create\", \"update\"]} \npath \"sys/namespaces/api-lock/unlock/+\" {capabilities = [\"create\", \"update\"]} \npath \"sys/namespaces/+\" {capabilities = [\"create\", \"update\", \"delete\", \"list\", \"read\"]} \npath \"+/sys/mounts/+\" {capabilities = [\"create\", \"update\", \"delete\", \"list\", \"read\"]}"

}'
```

Шаг 4: Создать парольную политику для namespace

```
curl --request POST \

  --url https://.... /v1/sys/policy/имя__политики_namespace \

  --header 'Content-Type: application/json' \

  --header 'X-Vault-Token: …' \

  --data '{
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
        "policy": "path \"+/sys/namespaces/api-lock/lock/+\" {capabilities = [\"create\", \"update\"]}
\npath \"+/sys/namespaces/api-lock/unlock/+\" {capabilities = [\"create\", \"update\"]} \npath
\"+/sys/namespaces/+\" {capabilities = [\"create\", \"update\", \"delete\", \"list\", \"read\"]} \npath
\"+/+/sys/mounts/+\" {capabilities = [\"create\", \"update\", \"delete\", \"list\", \"read\"]}"

    }'
```

Шаг 5: Выпустить токен для работы с тенантом

```
curl --request POST \
  --url https://.... /v1/auth/token/create \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "policies": [
          "имя__политики_тенанта"
    ],
    "ttl": "2h",
    "display_name": "имя__политики_тенанта",
    "type": "service"
}'
```

В выходных параметрах будет выдан токен для работы с тенантом

Шаг 6: Выпустить токен для работы с namespace

```
curl --request POST \
  --url https://.... /v1/auth/token/create \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "policies": [
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
            "имя__политики_namespace"
    ],
    "ttl": "2h",
    "display_name": "имя__политики_namespace",
    "type": "service"
}'
```

В выходных параметрах будет выдан токен для работы с namespace

Шаг 7: Создать движок секретов в тенанте

```
curl --request POST \
  --url https://.... /v1/имя_тенанта/sys/mounts/имя_движка \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
      "type": "kv"
}'
```

Шаг 8: Создать движок секретов в namespace

```
curl --request POST \
  --url https://.... /v1/имя_тенанта/имя_namespace/sys/mounts/имя_движка \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
      "type": "kv"
}'
```

Шаг 9: Архивировать namespace

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая
Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
curl --request POST \
  --url https://.... /v1/имя_тенанта/sys/namespaces/api-lock/lock/имя_namespace \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
}'
```

Шаг 10: Разархивировать namespace

```
curl --request POST \
  --url https://.... /v1/имя_тенанта/sys/namespaces/api-lock/unlock/имя_namespace \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
      "unlock_key": ""
}'
```

Шаг 11: Архивировать тенант

```
curl --request POST \
  --url https://.... /v1/sys/namespaces/api-lock/lock/имя_тенанта \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
}'
```

Шаг 12: Разархивировать тенант

```
curl --request POST \
  --url https://.... /v1/sys/namespaces/api-lock/unlock/имя_тенанта \
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
        "unlock_key": ""
}'
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

2. Движок секретов RedHat IDM

Указание начиная с какой версии: *с 13-го релиза*

Краткое описание:

1. Движок выполняет аутентификацию по протоколу Kerberos.
2. Обеспечивает управление учетными данными (пароли, кейтабы):
   a) генерацию секретов;
   b) ротацию секретов;
   c) удаление секретов;
   b) установку срока жизни секретов.
3. Система автоматически определять активные узлы кластера, доступные для выполнения требуемых операций, в том числе создания секретов, ротации секретов, удаления секретов

3. Движок секретов PostgreSQL

Указание начиная с какой версии: *с 13-го релиза*

Краткое описание:

1.Система выполняет аутентификацию по протоколам:

a. Kerberos
b. TLS

2.Система автоматически определяет активные узлы кластера, доступные для выполнения требуемых операций, в том числе создание секретов, ротации секретов, удаления секретов. Смена активного узла кластера не приводит к необходимости внесения изменений в систему или атрибутов сопутствующих секретов.

3.При настройке аутентификации системы и создания статических ролей, есть возможность выбора схемы ротации секрета такие как Pull и Push.

Описание настройки:

Предусловие: движок database активирован.

```
{
  "plugin_name": "postgresql-database-plugin",
  "allowed_roles": "*",
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

"connection_url": "postgres://{{username}}:{{password}}@hostname:port,hostname:port/имя_базы_данных?sslmode=require&target_session_attrs=read-write",

"credential_type": "password",

"verify_connection": "true",

"username": "Логин от УЗ, с правами на подключение к БД и смену паролей локальных УЗ",

"password": "Пароль от УЗ, под которой происходит аутентификация",

}

Шаги проверки:

Шаг 1: Активировать движок

```
curl --request POST \
  --url https://.... /v1/sys/mounts/имя_движка \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "type":"database"
}'
```

Шаг 2: Настроить движок

```
curl --request POST \
  --url https://.... /v1/имя_движка/config/имя_соединения \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    См. Описание настройки
}'
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Шаг 3: Создать статическую роль

```
curl --request POST \
  --url https://.... /v1/имя_движка/static-roles/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
   "db_name": "имя_соединения",
   "username":"Имя ТУЗ, которую необходимо взять под управление"
   "rotation_period":"300",
   "rotation_scheme": "push",
   "rotation_statements": [
      "ALTER USER {{username}} WITH PASSWORD ‘{{password}}’;"
   ]
}'
```

Шаг 4: Получить пароль статической роли

```
curl --request GET \
  --url https://.... /v1/имя_движка/static-creds/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
}'
```

В выходных параметрах будет выдан пароль

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая
Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

4. Движок секретов Oracle

Указание начиная с какой версии: *с 16-го релиза*

Краткое описание:

1. Система выполняет аутентификацию по протоколу TLS

2. Система автоматически определяет активные узлы кластера, доступные для выполнения требуемых операций, в том числе создание секретов, ротации секретов, удаления секретов. Смена активного узла кластера не приводит к необходимости внесения изменений в Систему или атрибутов сопутствующих секретов.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

5. Бесшовное обновление (graceful shutdown) + SDK

Указание начиная с какой версии: *с 12-го релиза*

Краткое описание:

Процесс бесшовного обновления проходит в штатном функционирующей системе (кластере Vault). Суть процесса заключается в последовательном выводе из эксплуатации серверов Vault устаревшей версии и замене их на серверы новой версии, с немедленным вводом в эксплуатацию.

1. Graceful shutdown(плавный вывод сервера Vault из балансировки):

Процесс вывода из балансировки не приводит к отказам при исполнении запросов.

Для реализации процесса вывода из балансировки было доработано программное обеспечение Vault:

- В части процесса передачи лидерства master-сервером.
- В части предоставления сведений о статусе работы сервера для устройств балансировки нагрузки и/или устройств типа API Gateway.

2. SDK:

Для обеспечения высокой доступности и непрерывности работы системы, на стороне клиента была обеспечена корректная обработка сообщений об ошибках и отсутствие ответов.

Общий алгоритм обработки всех ошибочных состояний включает в себя механизм повтора запроса после заданного времени задержки. Время задержки изменяется на случайную величину в большую или меньшую сторону на определенный процент.

3. Performance standby (быстрое переключение с ведомого на лидера):

Предварительно распакованные ноды кластера Vault. Для более быстрого смены мастера Vault. Те объекты и структуры, которые хранят все свои данные в кеше, должны быть инициализированы , при этом наполнение их не требуется - при переключении узла кластера , данные при первом обращении будут считаны из БД.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

6. Движок секретов OS Linux

Указание начиная с какой версии: *с 16-го релиза*

Краткое описание:

Плагин OS Linux способен:

1. Выполнять взаимодействие с серверами под управлением Linux или Unix с использованием SSH версии 2.
2. Поддерживать взаимодействие с:
    a. RHEL версий 7 и более новых;
    b. Ubuntu версий 12, 16 и более новых;
    c. AIX;
    d. Solaris.
3. Выполнять аутентификацию при взаимодействии с серверами под управлением Linux или Unix по протоколам:
    a. SSH с использованием логина и пароля УЗ Linux и\или Unix
    b. SSH с использованием логина и пароля УЗ RedHat IDM
    c. SSH с использованием ключей
4. Автоматически определять активные узлы кластера, доступные для выполнения требуемых операций, в том числе создания секретов, ротации секретов, удаления секретов.

7. Plugin для интеграции с собственными Удостоверяющими центрами Заказчика

Указание начиная с какой версии: *с 12-го релиза*

Краткое описание:

1. Плагин выполняет аутентификацию при взаимодействии с собственным Удостоверяющим центром заказчика по протоколу TLS.
2. Выполняет управление сертификатами:
    a) генерацию;
    b) ротацию;
    c) аннулирование;
3. Реализована возможность получения актуальных списков аннулированных сертификатов.
4. Обеспечена интеграция с центрами сертификации с возможность регистрации выпускаемых сертификатов в системе HP SM.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

8. Система Отчетности

Указание начиная с какой версии: *(отдельный компонент)*

Краткое описание:

Система Отчетности в коробочной версии Vault - отсутствует. Доработанная система:

1. получает данные из Active Directory о:
   - Группах
   - Пользователях
2. получает данные из Vault об:
   - Аутентификаторах (возможности аутентификации пользователей) и их политиках,
   - Политиках и их правилах
   - Секретах
3. собирает данные с нескольких стендов Vault и нескольких серверов Active Directory в том числе и из разных сетевых зон
4. предоставляет данные для считывания системой Qlik через протокол СУБД Postgres
5. Также Система Отчетности:
   - предоставляет отчет по всем секретам (с указанием различной информации, например владельца секрета)
   - позволяет указать фильтр, по которому можно выводить отчет
   - формирует отчет по запросу

Система отчетности состоит из 2 компонентов:

- Экстрактор
- Импортер и его БД

  Задача этих компонентов - доставка необходимых для построения отчета данных из Системы и Active Directory в БД Импортера. Имеется возможность интеграции с BI Qlik Sence для построения отчетов на основе собранных данных

9. Движок секретов SSH

Указание начиная с какой версии: *с 12-го релиза*

Краткое описание:

Движок генерации SSH-ключей способен выполнять операции по генерации ключей с различными форматами, алгоритмами генерации и размерами открытой части ключа для каждого из алгоритма.

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

Описание настройки:

Предусловие: движок sshkeygen активирован.

```
{
    "password_policy": "имя_парольной_политики"
}
```

Шаги проверки:

Шаг 1: Активировать движок

```
curl --request POST \
  --url https://.... /v1/sys/mounts/имя_движка \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "type":"sshkeygen"
}'
```

Шаг 2: Создание парольной политики:

```
curl --request POST \
  --url https://.... /v1/sys/policies/password/имя_парольной_политики \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "policy": "length = 25\nrule \"charset\" {\n charset = \"abcdefghjkmnopqrstuvwxyz\"\nmin-chars = 10}\nrule \"charset\" {\n charset = \"ABCDFGHIJKLMNPQRSTUVWXYZ\"\nmin-chars = 10}\nrule \"charset\" {\n charset = \"0123456789\"\nmin-chars = 3}\nrule \"charset\" {\n charset = \"!@#$%^&*\"\nmin-chars = 2}"
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

```
}'
```

Шаг 3: Настроить движок

```
curl --request POST \
  --url https://.... /v1/имя_движка/config \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
     См. Описание настройки
}
```

Шаг 4: Создать роль

```
curl --request POST \
  --url https://.... /v1/имя_движка/roles/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
    "key_algo": "rsa",
    "public_key_size":  2048,
    "format": "pem"
}'
```

Шаг 5: Сгенерировать SSH ключ

```
curl --request POST \
  --url https://.... /v1/имя_движка/keys/имя_роли \
  --header 'Content-Type: application/json' \
  --header 'X-Vault-Token: …' \
  --data '{
```

ООО «ЭйТи Консалтинг»,
127015, г. Москва, ул. Большая Новодмитровская, д. 14, стр. 7, офис 523

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
www.at-consulting.ru

}'

В выходных параметрах будет выдан ключ SSH (публичная и закрытая части)

10. Комплекты ТУЗ.

Указание начиная с какой версии: *с 14-го релиза*

Краткое описание: Система способна обеспечивать поддержку комплектов пар ТУЗ, состоящих из смещенных друг относительно друга ТУЗов и их секретов, по срокам действия. Таким образом при запросе параметров доступа будет выдаваться, а при доставке - доставляться актуальный секрет с гарантированным остаточным сроком действия. Соответственно, ротация секретов ТУЗ, настроена таким образом, чтобы ТУЗ и секреты для которых настроена доставка были актуальны на всех доступных ресурсах - источниках, их использующих.