Использование REST API Сервера интеграции в сценариях управления кластером Серверов интеграции

Kaspersky Security для виртуальных сред 6.4 Легкий агент

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

Содержание

Об использовании REST API Сервера интеграции

Вы можете использовать REST API Сервера интеграции в сценариях управления отказоустойчивым кластером Серверов интеграции на базе Linux.

Предварительно вам нужно выполнить установку и первоначальную настройку Серверов интеграции, которые будут выполнять роли главного и резервного Серверов интеграции. Серверы интеграции нужно установить на отдельных устройствах с операционной системой Linux (подробнее см. в справке Kaspersky Security для виртуальных сред 6.4 Легкий агент).

С помощью REST API Сервера интеграции вы можете выполнять следующие действия:

- Назначать роль главному Серверу интеграции.
- Добавлять сертификат резервного Сервера интеграции в список доверенных сертификатов главного Сервера интеграции.
- Регистрировать и отменять регистрацию резервных Серверов интеграции на главном Сервере интеграции.

Все процедуры нужно выполнять на Сервере интеграции, который выполняет роль главного Сервера интеграции в составе отказоустойчивого кластера Серверов интеграции.

Взаимодействие с REST API Сервера интеграции основано на запросах и ответах в формате json и осуществляется по протоколу HTTPS. Для взаимодействия с REST API Сервера интеграции требуется аутентификация на Сервере интеграции с использованием токена (bearer token).

Аутентификация на Сервере интеграции

Для аутентификации на Сервере интеграции используется подписанный сервером токен (bearer token). Вам нужно указывать следующий заголовок с токеном в каждом запросе REST API:

```
Authorization: Bearer <accessToken>
```

Чтобы получить токен, выполните запрос:

```
GET /api/3.0/auth/tokens
```

В заголовке этого запроса укажите имя пользователя admin и пароль администратора Сервера интеграции следующим образом:

```
Authorization: Basic <строка имя пользователя:пароль, закодированная методом Base64>
```

В результате успешного выполнения запроса возвращается код 200 и тело ответа:

```
{
  "accessToken": {
    "value": "<accessToken>"
  },
  "refreshToken": {
    "value": "<refresh_token>"
  },
  "session": {
    "id": "<session_id>",
    "createdAt": "<timestamp>",
    "updatedAt": "<timestamp>",
    "activeTo": "<timestamp>",
    "validTo": "<timestamp>"
  }
}
```

Токен, который нужно передавать в заголовке каждого запроса, содержится в значении поля “value” элемента "accessToken".

Назначение роли главному Серверу интеграции

По умолчанию все установленные Серверы интеграции имеют роль "одиночный". Вам нужно назначить одному из Серверов интеграции роль главного Сервера интеграции в отказоустойчивом кластере. Для этого на выбранном Сервере интеграции выполните запрос:

```
PUT /api/3.0/server/configuration/role
```

В теле запроса укажите следующие параметры:

```
{
  "role": "Primary",
}
```

В результате успешного выполнения запроса возвращается код 200 с пустым телом ответа.

Добавление сертификата резервного Сервера интеграции на главный Сервер интеграции

Для успешной регистрации и подключения резервного Сервера интеграции к главному Серверу интеграции вам нужно добавить сертификат резервного Сервера интеграции в список доверенных сертификатов главного Сервера интеграции. Для этого:

1. Получите сертификат резервного Сервера интеграции с помощью запроса:

   `GET /api/3.0/sslConfig/getCertificate?address=<address>:<port>`

   где:

   - <address> – адрес резервного Сервера интеграции.
   - <port> – порт для подключения к резервному Серверу интеграции.

   В результате успешного выполнения запроса возвращается следующий ответ:

```
{
  "address": "<address>:<port>",
  "thumbprint": "<thumbprint>",
  "data": "<data>",
  "viisValidationResult": {
      "isAccepted": true,
      "validationWarnings": [],
      "validationErrors": []
  }
}
```

   где:

   - <address>:<port> – адрес и порт резервного Сервера интеграции, указанные в запросе.
   - <thumbprint> – отпечаток сертификата, который вам нужно добавить в список доверенных сертификатов главного Сервера интеграции.
   - <data> – тело полученного сертификата, на основе которого можно построить и проверить полученный сертификат.

2. Добавьте сертификат в список доверенных сертификатов главного Сервера интеграции с помощью запроса:

   `POST /api/3.0/sslConfig/certificateValidator/rules`

   В теле запроса укажите следующие параметры:

```
{
  "address": "<address>:<port>",
  "thumbprint": "<thumbprint>"
}
```

где:

- <address>:<port> – адрес и порт резервного Сервера интеграции, которые вы указали в запросе на получение сертификата.
- <thumbprint> – отпечаток сертификата, полученный в результате выполнения запроса на получение сертификата.

В результате успешного выполнения запроса возвращается код 201 с пустым телом ответа.

Управление резервными Серверами интеграции

Для управления резервными Серверами интеграции предусмотрены следующие процедуры:

- Регистрация резервного Сервера интеграции на главном Сервере интеграции.
- Обновление параметров ранее зарегистрированного резервного Сервера интеграции.
- Получение списка зарегистрированных резервных Серверов интеграции.
- Отмена регистрации резервного Сервера интеграции на главном Сервере интеграции.

Регистрация резервного Сервера интеграции на главном Сервере интеграции

Вам нужно выполнить процедуру регистрации для назначения Серверу интеграции роли "резервный" и настройки взаимодействия главного и резервного Серверов интеграции.

Зарегистрированному Серверу интеграции назначается роль "резервный". В результате назначения роли "резервный" на Сервере интеграции становится доступна функция получения информации о виртуальной инфраструктуре с главного Сервера интеграции и функция предоставления Легким агентам информации об SVM в случае недоступности главного Сервера интеграции. Другие функции Сервера интеграции блокируются для резервного Сервера интеграции.

Чтобы зарегистрировать резервный Сервер интеграции на главном Сервере интеграции, выполните запрос:

```
POST /api/3.0/ha/instances
```

В теле запроса укажите следующие параметры:

```
{
  "role": "Reserve",
  "address": "<address>:<port>"
  "password": "<admin password>"
}
```

где:

- <address>:<port> – адрес и порт резервного Сервера интеграции.
- <admin password> – пароль администратора Сервера интеграции, закодированный методом Base64.

В результате успешного выполнения запроса в теле ответа возвращается идентификатор резервного Сервера интеграции (<reserve VIIS ID>) и информация о статусе подключения к главному Серверу интеграции:

```
{
  "createdAt": "<timestamp>",
  "id": "<reserve VIIS ID>",
```

```
  "role": "Reserve",
  "address": "<address>:<port>",
  "connectionInfo": {
    "status": "<connection status>",
    "connectionError": "<error>"
  }
}
```

где:

- <reserve VIIS ID> – идентификатор резервного Сервера интеграции.
- <address>:<port> – адрес и порт резервного Сервера интеграции.
- <connection status>– текущий статус подключения резервного Сервера интеграции к главному Серверу интеграции. Возможные значения: Connecting | Connected | Disconnected.
- <error> – информация об ошибке подключения. Возможные значения: NoError | ServerError | NetworkError | InvalidCertificate | AccessDenied | Unauthorized.

Процесс подключения занимает некоторое время, дождитесь успешного завершения подключения.

Чтобы посмотреть текущий статус подключения, выполните запрос:

```
GET /api/3.0/ha/instances/<reserve VIIS ID>
```

Резервный Сервер интеграции считается зарегистрированным, если в элементе "connectionInfo" поле "status" имеет значение "Connected".

Обновление параметров резервного Сервера интеграции

Эта процедура может потребоваться, если у резервного Сервера интеграции изменился адрес. Вместо того, чтобы отменять регистрацию Сервера интеграции и затем снова регистрировать его на главном Сервере интеграции, вы можете выполнять процедуру обновления параметров.

Чтобы обновить параметры резервного Сервера интеграции, выполните запрос:

```
PUT /api/3.0/ha/instances/<reserve VIIS ID>
```

где <reserve VIIS ID> – идентификатор резервного Сервера интеграции, полученный в результате его регистрации на главном Сервере интеграции.

В теле запроса укажите следующие параметры:

```
{
  "role": "Reserve",
  "address": "<address>:<port>"
  "password": "<admin password>"
}
```

где:

- <address>:<port> – актуальные адрес и порт резервного Сервера интеграции.
- <admin password> – пароль администратора Сервера интеграции, закодированный методом Base64.

В результате успешного выполнения запроса в теле ответа возвращается идентификатор резервного Сервера интеграции (<reserve VIIS ID>) и информация о статусе подключения к главному Серверу интеграции:

```
{
  "createdAt": "<timestamp>",
  "id": "<reserve VIIS ID>",
  "role": "Reserve",
  "address": "<address>:<port>",
  "connectionInfo": {
    "status": "<connection status>",
    "connectionError": "<error>"
  }
}
```

где:

- <connection status>– текущий статус подключения резервного Сервера интеграции к главному Серверу интеграции. Возможные значения: Connecting | Connected | Disconnected.
- <error> – информация об ошибке подключения. Возможные значения: NoError | ServerError | NetworkError | InvalidCertificate | AccessDenied | Unauthorized.

Процесс подключения занимает некоторое время, дождитесь успешного завершения подключения.

Чтобы посмотреть текущий статус подключения, выполните запрос:

```
GET /api/3.0/ha/instances/<reserve VIIS ID>
```

Параметры резервного Сервера интеграции обновлены, если в элементе "connectionInfo" поле "status" имеет значение "Connected".

Получение списка резервных Серверов интеграции

Чтобы получить список зарегистрированных резервных Серверов интеграции, выполните запрос:

```
GET /api/3.0/ha/instances
```

> В Kaspersky Security для виртуальных сред Легкий агент версии 6.4 на главном Сервере интеграции может быть зарегистрирован только один резервный Сервер интеграции.

В результате успешного выполнения запроса возвращается следующий ответ:

```
{
    "instances": [
        {
            "createdAt": "<timestamp>",
            "id": "<reserve VIIS ID>",
            "role": "Reserve",
```

```
            "address": "<address>:<port>",
            "connectionInfo": {
                "status": "<connection status>",
                "connectionError": "<error>"
            }
        }
    ]
}
```

Отмена регистрации резервного Сервера интеграции на главном Сервере интеграции

Чтобы отменить регистрацию резервного Сервера интеграции, выполните запрос:

```
DELETE /api/3.0/ha/instances/<reserve VIIS ID>
```

где <reserve VIIS ID> – идентификатор резервного Сервера интеграции, полученный в результате его регистрации на главном Сервере интеграции.

В результате успешного выполнения запроса возвращается код 200 с пустым телом ответа.