Using the Integration Server REST API in Integration Server cluster management scenarios

Kaspersky Security for Virtualization 6.4 Light Agent

Dear user,

Thank you for trusting us. We hope that this document helps you in your work and answers most of your questions.

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

Learn about Kaspersky at https://www.kaspersky.com/about/company

Contents

Using the Integration Server REST API

You can use the Integration Server REST API in scenarios involving the management of a high-availability cluster of Linux-based Integration Servers.

Before you start, you need to complete the installation and initial configuration of the Integration Servers that will act as the primary and reserve Integration Servers. The Integration Servers must be installed on separate Linux devices (for details, see the Kaspersky Security for Virtualization 6.4 Light Agent Help).

You can use the Integration Server REST API to do the following:

- Assign the primary Integration Server role.
- Add the certificate of the reserve Integration Server certificate to the list of trusted certificates on the primary Integration Server.
- Register and de-register reserve Integration Servers with the primary Integration Server.

All procedures must be performed on the Integration Server that is acting as the primary Integration Server in the high-availability cluster of Integration Servers.

Interaction with the Integration Server REST API is based on requests and responses in JSON format and is carried out over the HTTPS protocol. To interact with the Integration Server REST API, authentication on the Integration Server using a bearer token is required.

Authentication on the Integration Server

A server-signed token (bearer token) is used to authenticate on the Integration Server. In each REST API request, you need to specify the following header with the token:

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

To get the token, make the following request:

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

In the header of this request, specify the user name "admin" and the password of the Integration Server administrator as follows:

```
Authorization: Basic <Base64-encoded username:password string>
```

If the request succeeds, a 200 code and a response body are returned:

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

The token, which must be sent in the header of each request, is contained in the "value" field of the "accessToken" element.

Assigning a role to the primary Integration Server

By default, all installed Integration Servers have the "standalone" role. You need to assign the primary Integration Server role in the high-availability cluster to one of the Integration Servers. To do this, make the following request on the chosen Integration Server:

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

Specify the following parameters in the request body:

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

If the request succeeds, a 200 code and empty response body are returned:

Adding the certificate of the reserve Integration Server to the primary Integration Server

To have the reserve Integration Server connect to and register with the primary Integration Server, you need to add the certificate of the reserve Integration Server to the list of trusted certificates on the primary Integration Server. To do this:

1. Get the certificate of the reserve Integration Server using the following request:

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

   where:

   - <address> is the address of the reserve Integration Server.
   - <port> is the port for connecting to the Integration Server.

   If the request succeeds, the following response is returned:

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

   where:

   - <address>:<port> is the address and port of the reserve Integration Server specified in the request.
   - <thumbprint> is the thumbprint of the certificate that you need to add to the list of trusted certificates on the primary Integration Server.
   - <data> is the body of the received certificate, which is used to build and verify the received certificate.

2. Add the certificate to the list of trusted certificates on the primary Integration Server using the following request:

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

   Specify the following parameters in the request body:

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

where:

- <address>:<port> is the address and port of the reserve Integration Server that you specified in the certificate request.
- <thumbprint> is the certificate thumbprint received in response to the certificate request.

If the request succeeds, a 201 code and empty response body are returned:

Managing reserve Integration Servers

The following procedures are provided for managing reserve Integration Servers:

- Registering a reserve Integration Server with the primary Integration Server
- Updating the settings of a previously registered reserve Integration Server
- Getting a list of registered reserve Integration Servers
- De-registering a reserve Integration Server on the primary Integration Server

Registering a reserve Integration Server with the primary Integration Server

You need to complete the registration procedure to assign the "reserve" role to the Integration Server and configure the interaction between the primary and reserve Integration Servers.

A registered Integration Server gets the "reserve" role. The Integration Server with the "reserve" role can get information about the virtual infrastructure from the primary Integration Server and provide information about SVMs to Light Agents whenever the primary Integration Server is unavailable. The rest of the Integration Server functions are blocked for the reserve Integration Server.

To register the reserve Integration Server with the primary Integration Server, execute the following request:

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

Specify the following parameters in the request body:

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

where:

- <address>:<port> is the address and port of the reserve Integration Server.
- <admin password> is the Base64-encoded password of the Integration Server administrator.

As a result of successful execution of the request, ID of the reserve Integration Server (<reserve VIIS ID>) is returned in the response body, as well as information about the status of connection to the primary Integration Server:

```
{
  "createdAt": "<timestamp>",
  "id": "<reserve VIIS ID>",
  "role": "Reserve",
  "address": "<address>:<port>",
  "connectionInfo": {
```

```
    "status": "<connection status>",
    "connectionError": "<error>"
  }
}
```

where:

- <reserve VIIS ID> is the ID of the reserve Integration Server.
- <address>:<port> is the address and port of the reserve Integration Server.
- <connection status> is current status of the connection of the reserve Integration Server to the primary Integration Server. Possible values: Connecting | Connected | Disconnected.
- <error> is information about a connection error. Possible values: NoError | ServerError | NetworkError | InvalidCertificate | AccessDenied | Unauthorized.

The connection process takes some time; please wait until the connection is successfully established.

To view the current connection status, make the following request:

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

The reserve Integration Server is registered if the value of the "status" field in the "connectionInfo" element is "Connected".

Updating the settings of a reserve Integration Server

You may need to follow these steps if the address of the reserve Integration Server has changed. Instead of de-registering the Integration Server and then registering it again with the primary Integration Server, you can follow the steps to update settings.

To update the settings of the reserve Integration Server, make the following request:

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

where <reserve VIIS ID> is the ID of the reserve Integration Server obtained as a result of its registration with the primary Integration Server.

Specify the following parameters in the request body:

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

where:

- <address>:<port> is the current address and port of the reserve Integration Server.
- <admin password> is the Base64-encoded password of the Integration Server administrator.

As a result of successful execution of the request, ID of the reserve Integration Server (<reserve VIIS ID>) is returned in the response body, as well as information about the status of connection to the primary Integration Server:

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

where:

- <connection status> is current status of the connection of the reserve Integration Server to the primary Integration Server. Possible values: Connecting | Connected | Disconnected.
- <error> is information about a connection error. Possible values: NoError | ServerError | NetworkError | InvalidCertificate | AccessDenied | Unauthorized.

The connection process takes some time; please wait until the connection is successfully established.

To view the current connection status, make the following request:

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

The settings of the reserve Integration Server are updated if the value of the "status" field in the "connectionInfo" element is "Connected".

Getting a list of reserve Integration Servers

To get a list of registered reserve Integration Servers, make the following request:

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

> In Kaspersky Security for Virtualization 6.4 Light Agent, only one reserve Integration Server can be registered with the primary Integration Server.

If the request succeeds, the following response is returned:

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

De-registering a reserve Integration Server on the primary Integration Server

To de-register a reserve Integration Server, make the following request:

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

where <reserve VIIS ID> is the ID of the reserve Integration Server obtained as a result of its registration with the primary Integration Server.

If the request succeeds, a 200 code and empty response body are returned: