IBM Verify Gateway for RADIUS

Contents

IBM Verify Gateway for RADIUS

Roadmap

1. Ensure that you met all the requirements. See "Prerequisites."
2. Install the IBM® Verify Gateway for RADIUS. See "Installing the IBM Verify Gateway for RADIUS server."
3. Configure the IBM Verify Gateway for RADIUS. See "Configuring the IBM Verify Gateway for RADIUS server" on page 2.
4. Starting the server. See "Start the service" on page 12.
5. Uninstalling the server. See "Uninstalling the IBM Verify Gateway for RADIUS server" on page 13.

Prerequisites

Operating System requirements

Windows Server 2012 through Windows Server 2016, 64-bit

System requirements

Minimum Windows Server OS system requirements specific to the actual OS version.

Network requirements

- Port 443 open to the Cloud Identity tenant address (TLS).
- Port 1812 inbound from RADIUS Client server's UDP. Communication over UDP between the IBM Verify Gateway for RADIUS and the RADIUS client must be through the configured RADIUS server port. The default RADIUS server port is 1812.

VC_redist.x64.exe

Microsoft Visual C++ 2017 Redistributable (x64) version 14.14.26429

This file can be obtained directly from the MSDN web site `https://go.microsoft.com/fwlink/?LinkId=746572`.

Microsoft .NET Framework 4.6.1

If not installed, the IBM Verify Gateway for RADIUS installer (`setup.exe`) automatically initiates the download of the Microsoft .NET Framework from the Microsoft website.

Installing the IBM Verify Gateway for RADIUS server

Before you begin

You need the `IbmRadiusInstaller.msi` that is provided with the IBM Verify Gateway for RADIUS.

About this task

Procedure

1. Copy the following two files onto the Windows server disk.
   - `Setup.exe`
   - `IbmRadiusInstaller.msi`
2. If not already installed on the system, download and run the `VC_redist.x64.exe` file from the link in "Prerequisites."
3. Run the `Setup.exe` file.

4. Accept the defaults and complete the Verify Gateway for RADIUS installation. The Windows Server file system contains the following files in the `C:\Program Files\ibm\IbmRadius` directory:

   ```
   cacert.pem
   cacert.pem.sample
   cJSON.dll
   IbmAuthApi.dll
   IbmRadius.exe
   IbmRadiusConfig.json
   IbmRadiusConfig.json.sample
   IbmRadiusMsg.dll
   libcurl.dll
   LIBEAY32.dll
   SSLEAY32.dll
   zlib1.dll
   ```

   A Windows service is set up for `IbmRadius.exe` with name "IBM RADIUS Service". It's not running and the startup type is set to "Manual".

   Note: A license folder is included under the main installation directory. It includes the associated licenses and notices in the supported languages.

Configuring the IBM Verify Gateway for RADIUS server

About this task

Procedure

1. Create API client credentials.
   a. Log in to the IBM Cloud Identity administration console.
   b. Click **Settings** > **API Access** > **Add API Client** > **.**
   c. Provide a name for the client. For example, IBM Verify Gateway.
   d. Select the check boxes to grant the following access rights.

      Authenticate any user
      Manage second-factor authentication enrollment for all users
      Manage users and groups
      Read second-factor authentication enrollment for all users
      Read second-factor authentication method configuration
      Read users and groups

   e. Click **Save**.
   f. Locate your API client in the list and hover the end of the row to display the edit icon.
   g. Click the edit icon The API client information is displayed.
   h. Copy the Client ID and Secret to the clipboard or click the eye icon to view the secret and save the information. You will need this information when you edit the `IbmRadius` configuration file.
   i. Click **Cancel**. No changes are necessary.

   For more information, see Managing API clients.
2. Create users.
   a. Use the IBM Cloud Identity administration console to create users for the Verify Gateway for RADIUS server. See Managing users.

For each user that requires second-factor authentication, you must enroll them for OTP such as TOTP, EmailOTP or SMSOTP through the relevant enrollment APIs in Cloud Identity Verify.

Note: The IBM RADIUS server product does not provide a function for enrolling users for OTP.

3. Edit the `IbmRadius` configuration file. The `IbmRadiusConfig.json` file is of JSON format with one enhancement, you can comment out areas of the file by wrapping them between `/*` and `*/`.

   See https://www.json.org/ for the JSON.

   a. Edit the `C:\Program Files\ibm\IbmRadius\IbmRadiusConfig.json` file with your favorite text file editor. In this quick example, replace the *variable* values with the Client ID and Client Secret determined in 1h on page 2 and update the host name of the IBM Cloud Identity server that is being used and the Client IP of the Verify Gateway for RADIUS client to be used.

      Update the client address to match your Verify Gateway for RADIUS client (NAS) address, such as a VPN server or PAM RADIUS module. The RADIUS client will need to be configured with the Client Secret value that you set in this file.

```
{
   "address": "::",
   "port": 1812,
   "ibm-auth-api": {
      "host": "xxxxxxxx.ice.ibmcloud.com",
      "max-handles": 16,
      "protocol": "https",
      "port": 443,
      "client-id": "xxxxxxxx",
      "client-secret": "xxxxxxxx"
   },
   "policy" : [
      {
         "name": "policy1",
         "return-attrs": [
            {
               "value": "Login",
               "name": "Service-Type"
            }
         ]
      }
   ],
   "clients": [
      {
         "address": "192.168.1.144",
         "mask": "255.255.255.255",
         "choice-prompt": "Please select an authentication method from the list: \r\n",
         "identity-source": "869e5652-bbb1-4f9b-8e55-0ae53d3bc30b",
         "auth-method": "password-then-totp",
         "name": "client1",
         "transients-in-choice": false,
         "transient-choices": ["emails", "phoneNumbers"],
         "use-external-ldap": true,
         "choice-line-prompt": "Enter %I for %D \r\n",
         "secret": "passw0rd",
         "no-devices-in-choice": false,
         "reject-on-missing-auth-method": false,
         "no-enrollments-in-choice": false,
         "device-prompt": "A push notification has been sent to your device: [%D].",
         "poll-device": true,
         "poll-timeout": 60
      }
   ]
}
```

   b. Edit the top level {} section. It that contains the Verify Gateway for RADIUS global settings. See "Top level {}" on page 4.

c. Edit the "ibm-auth-api": {} section. It contains the connection details to the IBM Cloud Identity server. See “"ibm-auth-api":{}.”
d. Edit the "clients": [] section. It contains the connection details to the IBM Cloud Identity server. See “"clients":[]” on page 5.
e. Edit the "policy":[] section. It is an array of policies that can conditionally add attributes, or accept or approve authorization requests. See “"policy":[]” on page 9.

Top level {}

This section contains the Verify Gateway for RADIUS server global settings.

Format

```
{
  "address":"xxx",
  "port":xxx,
  "trace-file":"xxx",

  "ibm-auth-api":{
  ...
  },

  "clients":[
    ...
  ],

  "policy":[
    ...
  ]
}
```

Values:

"address":"::"

Specifies the list of up to 10 IP address for RADIUS requests. The value of “::” means all IPv6 and IPv4 addresses on the local computer. You might use “0.0.0.0” for all IPv4 addresses. Or you might specify a particular interface's address, such as “192.168.0.128”.

"port":"1812"

Specifies the IP port on which to listen for RADIUS requests. Port 1812 is the new RADIUS standard port for authentication.

/*"tace-file":"c:/tmp/ibm-auth-api.log"

Specifies a file to output low-level trace into for debugging issues. If you use the \ separator, then you must double each occurrence because the backslash has special meaning in JSON files, for example

```
"trace-file":"c:\\tmp\\ibm-auth-api"
```

Note:

This configuration item is commented out, the comments can be removed if the entry needs to be set.

"ibm-auth-api":{}

This section configures the connection to the Cloud Identity Verify server.

Format

```
"ibm-auth-api":{
  "client-id":"xxx",
  "client-secret":"xxx",
```

```
  ...
}
```

Values:

"client-id":"84e8da25-d7ed-47cc-9782-b852cb64365c"

This value is required. An IBM Cloud Identity API client must be created for use by the IBM Verify Gateway for RADIUS server. See “Configuring the IBM Verify Gateway for RADIUS server” on page 2 for the access settings it requires. An example of a client-id might be

```
"84e8da25-d7ed-47cc-9782-b852cb64365c"
```

.

“client-secret”:"XOpiba1XeP"

This value is required. The IBM Cloud Identity API client is given a password when it is created and must be set in this configuration setting. An example of a client-secret might be

```
XOpiba1XeP
```

.

Note: This client-secret can be set in an obfuscated form. Use the `IbmRadius.exe -obf <password>` command to generate the obfuscated version and use the alternate setting:

```
"obf-client-secret":"KsjKZsKrbbgNaPe7+kYIcOyWzZdzYNtF4KlCyYoNEFA=",
```

.

"protocol":"https"

This value is optional and defaults to “https”. This protocol is used to communicate to the IBM Cloud Identity server. Either value, “http” or “https”, can be used. When https is used and the `cacert.pem` file is present, the IBM Cloud Identity server certificate and server name are validated.

"host":"slick.ice.ibmcloud.com"

This value is required. It identifies the IBM Cloud Identity server that you are using.

"port":443

This value is optional and defaults to 443. This port is the port that the IBM Cloud Identity server is listening on for requests.

"max-handles":16

This value is optional and defaults to 16. This value is the maximum number of parallel connections that the IBM Verify Gateway for RADIUS server makes to the IBM Cloud Identity server for user authentication.

"clients":[]

The section is an array that contains details about each RADIUS client (NAS) that uses this RADIUS server.

Format

```
"clients":[
  {
    "name":"client1",
    "client-id":"xxx",
    ...
  },
```

```
  {
    "name":"client2",
    "client-id":"xxx",
    ...
  },
  ...
]
```

Values

“clients”:

One or more RADIUS clients (NAS) can be added to this array. All RADIUS clients that need to access this IBM RADIUS server must be listed by IP address in this array.

"secret":"passw0rd"

This value is required. This password is the shared secret between the IBM RADIUS server and the RADIUS client (NAS). It's used to encrypt passwords and sign response packets between the two.

Note: This client-secret can be set in an obfuscated form. Use the `IbmRadius.exe -obf <password>` command to generate the obfuscated version and use the alternate setting:

```
"obf-client-secret":"KsjKZsKrbbgNaPe7+kYIcOyWzZdzYNtF4KlCyYoNEFA=",
```

.

"address":"192.168.0.129"

This value is required. This address is the IP address packets from the RADIUS client (NAS) will appear to come from, and to where the responses are returned. It's used to match the RADIUS client (NAS) to the appropriate secret value.

"mask": "255.255.255.255"

This value is optional and defaults to `"255.255.255.255"`. This setting is a netmask that, in conjunction with the `"address"` configuration setting, is used to match an incoming client to a RADIUS client. A mask of `"255.255.255.255"` means that an incoming client must have the exact same IP address as the `"address"` to be matched. A mask of `"0.0.0.0"` means that any incoming client might be matched to this client. A mask of `"255.255.0.0"` matches incoming clients whose first two IP address octets matched those in `"address"`. If there are multiple matching clients, the match that has the "more specific" mask is chosen. For example, for two clients:

```
Client1 address: 192.168.0.0, mask: 255.255.255.0

Client2 address: 192.168.0.1, mask: 255.255.255.255
```

- If the incoming client address is `192.168.0.1`, then it would match Client2.
- If the incoming client address is `192.168.0.2`, then it would match Client1.
- If the incoming client address is `192.168.1.1`, then it would not match any client.

"auth-method":"password-then-smsotp"

This value is optional and defaults to `"password"`. This method is the method of authentication that is required to authenticate users. Acceptable values are as follows:

Table 1. Accepted values

Value	Description
password	Only a valid password is required.

Table 1. Accepted values (continued)

Value	Description
password-and-totp	A password plus a TOTP value must be provided in a single value. You can configure whether the password or the TOTP value is first in the value. See the `password-first` setting. To configure the character that is used to separate the two values, see the `password-separator` setting.
password-then-totp	After providing a valid password, a subsequent RADIUS challenge is sent that requests the TOTP value.
password-then-smsotp	After providing a valid password, an SMS message is sent to the user's registered mobile device with an OTP value. Then a RADIUS challenge is sent that requests the SMSOTP value.
password-then-emailotp	After providing a valid password, an email message is sent to the user with an OTP value. Then a RADIUS challenge is sent that requests the EmailOTP value.
password-then-transsmsotp	After providing a valid password, an SMS message with an OTP value is sent to the phone number in the user's profile. A RADIUS challenge is sent that requests the OTP value. Unlike `password-then-smsotp`, the user's phone number does not need to be enrolled for SMS OTP
password-then-transemailotp	After providing a valid password, an email message with an OTP value is sent to the email address in the user's profile. A RADIUS challenge is sent requesting the OTP value. Unlike `password-then-emailotp`, the user's email address does not need to be enrolled for email OTP.
password-then-choice-then-otp	After providing a valid password, a RADIUS challenge is sent that requests a choice of one of the user's OTP enrollments to use. After the choice is sent, a RADIUS challenge is sent that requests the OTP value for the choice. **Note:** If the user is only enrolled in one OTP method, then the choice challenge step is skipped and the user is challenged directly for the OTP value. If the user has no OTP enrollments, then reject-on-missing-auth-method comes into effect.

Table 1. Accepted values (continued)

Value	Description
password-and-device	After providing a valid password, a RADIUS challenge is sent that requests a choice of one of the user's valid registered devices to use. After the choice of device is sent, a RADIUS challenge is sent that corresponds to the highest priority authentication mechanism that is supported by the device. **Note:** • Authentication mechanisms, such as, Face, Fingerprint, or User Presence, are configurable by the administrator. If more than one mechanism is enabled, they are handled in an order of priority. The mechanism of greatest priority that is supported by the selected device is always chosen. • For a registered device to be valid, it must support at least one valid authentication mechanism that is configured by the administrator. • If only one registered device that supports the valid mechanisms exists, then the device choice step is skipped. The user is challenged with the priority mechanism for that device. • If no registered devices that support the valid mechanisms exist, then a REJECT response is issued.

"password-first":"false"
This value is optional and defaults to `false`. This setting controls whether the password is the first value in the password-separator-OTP concacentation that is submitted by the user for the password-and-totp authentication method.

For example, the OTP value is `1234`, the user's password is `Password`, and the separator character is `:`. If password-first is set to false, the user enters "1234:Password". If password-first is set to true, the user enters "Password:1234".

The separator character can be configured with the password-separator setting.

"password-separator":":"
This value is optional and defaults to `:`. This setting configures the character used to separate the password and OTP values that are submitted by the user for the `"password-and-totp"` auth-method.

"no-devices-in-choice":"true"
This value is optional and defaults to `false`. If set to `true`, the user's IBM Verify devices are not presented as authentication method choices.

"reject-on-missing-auth-method":"false"
This value is optional and defaults to `true`. If set to `false`, and the user is not registered for second factor OTP, then the user is not prompted for it and will be successfully authenticated. If set to `true`, and the user is not registered for second factor OTP, then the user will not be authenticated.

"otp-prompt":"Enter OTP %C:"
This value is optional and defaults to the English string `"Enter OTP %C: "`. This string is returned in the RADIUS challenge packet in the put into the RADIUS response packet variable `"Reply-Message" (18)`. Many RADIUS clients (NAS) show this string when requesting the input from the user. Any `%C` in the prompt is replaced by the OTP correlation, or the empty string for TOTP. Any `%%` in the prompt will be replaced by a single `%`.

"use-external-ldap":"false"
: This value is optional and defaults to `false`. Users are authenticated against a configured LDAP Pass-Through identity source. When set to `true` the `"identity-source"` value must be specified.

"identity-source":"869e5652-bbb1-4f9b-8e55-0ae53d3bc30b"
: This value is only required when `"use-external-ldap"` is set to `true`, it's otherwise optional. It specifies the identity source to be used to authenticate users. A collection of configured identity sources and their IDs can be retrieved from a GET request to `https://<tenant>/verify/v1.0/authnmethods/password` .

"choice-prompt":"Please select an authentication method from the list: \r\n"
: This value is optional. It defaults to the empty string: `""`. It allows a prefix to the choice line prompts to be configured. The choice line prompts and their prefixes are displayed when the user is required to choose an authentication method.

"choice-line-prompt":"Enter %I for %D \r\n"
: This value is optional. It allows each choice in the choice prompt to be customized. A choice prompt is generated for each choice that is available to the user. The default is `"%I) %D\r\n"`, where `%I` is replaced by the character that selects the choice, and `%D` is the choice description.

"device-prompt":"A push notification has been sent to your device: [%D]. "
: This value is optional. It allows the **`device/fingerprint/userpresence`** prompt to be customized. The default is `"A push notification has been sent to your device [%D]. Please refresh your IBM Verify application if you did not receive it."` , where `%D` is replaced by the device description.

"transients-in-choice":"false"
: If the "transients-in-choice" configuration line is set to `"true"`, then the OTP authentication choices listed in `"transient-choices"` based on the attributes from a user's cloud directory profile are included as OTP authentication choices, regardless of whether they're enrolled to receive SMS or email OTPs.

"transient-choices": ["emails", "phoneNumbers"]
: This value is optional. It defaults to `["emails","phoneNumbers"]`. This setting controls which transient OTP authentication choices are available to users.

"no-enrollments-in-choice":"false"
: This value is optional. It defaults to `false`. If the "no-enrollments-in-choice" configuration line is set to `"true"`, then the user's enrolled OTP methods including TOTP, email, and SMS are not included as authentication choices.

"poll-device":"false"
: This value is optional. It defaults to `false`. If set to `true`, then the server polls Cloud Identity Verify for a verification's state instead of prompting the user and waiting for the response.

"poll-timeout":"60"
: This value is optional. It defaults to `60`. This attribute sets the maximum number of seconds that the server polls Cloud Identity Verify, after a device verification is created. It has no effect if `"poll-device"` is set to `false`.

"policy":[]

This section is optional. It allows the conditional addition of attributes to the Access-Accept response packet from the IBM RADIUS server to RADIUS clients (NAS) and also allows the conditional immediate acceptance or rejection of an Access-Request authorization request. The policies are evaluated in the order that they are defined.

Format

```
"policy":[
  {
    "name":"policy1",
```

```
    "match":{
      "client-ip":"???",
      "attr":{
        "compare":"??",
        "name":"???",
         ...
      },
      "user-group":{
        "compare":"??",
        "name": "???"
      },
      "apply-before-authenticate":????
    },
    "return-attrs":[
      {
        "name":"???",
        "value":"???",
        ...
      },
      ...
    ],
    "action":"???",
  },
  {
    "name":"policy2",
    ...
  },
  ...
]
```

Values

"match":{}

This subsection is optional and if not present the policy matches all Access-Request packets.

Under this section, are the following subitems:

"client-ip":"192.168.0.129"

Optional. Matches the address of the RADIUS client (NAS) that sent the packet.

"apply-before-authenticate":"false"

Optional. Defaults to false. If true, the policy is matched and applied before the user password or OTP is validated.

"attr":{}

Optional. This section allows matching a single attributes value in the Access-Request. Under this section are the following subitems:

"compare":"="

Optional, defaults to "=". This item must be either `"="` or `"!="`.

"case-ignore":"false"

Optional, defaults to false. Values are compared based on a byte-by-byte comparison against the RADIUS attribute value. The exception is when `"case-ignore"` is set to true. For that case, a UTF-8 case-insensitive character string compare is done, which can be useful for comparing the `"User-Name"` attribute value.

"name":"User-Name"

The attribute in the Access-Request to compare to. This value can either be a string, such as a name for the RADIUS attribute, or the attribute number. For example, User-Name has the number 1. See the output of the **IbmRadius.exe -attributes** command for a list of RADIUS attributes.

"value":"Administrator"

The attribute value to compare with. See the following `"value-type"` table for the JSON format of the value. The default value type of the attribute depends on the attribute itself. The output of the command

```
"IbmRadius.exe
      -attributes"
```

shows the value-type of each RADIUS attribute.

"value-type":"text"

Optional. Overrides how the `"value"` is converted into a RADIUS attribute value. The default depends on the RADIUS attribute as each has its own default value-type. See the output of the **`IbmRadius.exe -attributes`** command to see the value-type of each RADIUS attribute. This parameter allows overriding of the type for ease of input. For example, a text string can be placed in a binary string attribute.

Table 2. Value mapping

Name	JSON value format	RADIUS Value
integer	number: for example, 1234 string:hex number, for example `"0xa2b3ff"`	4 bytes, MSB first
enum	string: enum name string appropriate for the attribute. For example, `"Login"` for the"“Service-Type" attribute. See the output of the **`IbmRadius.exe -attributes`** command for a list of acceptable enum value strings. number: for example,`5`	4 bytes, MSB first
time	number: number of seconds since 1970-01-01 00:00:00 UTC string: "YYYYMMDDHHMMSS" UTC	4 bytes, MSB first
text	string: UTF-8 characters	UTF-8 bytes not terminated by 0x00
integer64	number: for example, 12345 string:hex number, for example`"0xdeadbeaf"`	8 bytes, MSB first
ipv4addr	string: IPv4 formatted string, for example,`"192.168.0.1"`	4 bytes, network order, MSB first
ipv6addr	string: 6IPv4 formatted string, for example,`"192.168.0.fe80::df3c:99dd:8a4a:16f1"`	8 bytes, network order, MSB first
string ifid ipv6prefix ipv4prefix tlv vsa extended long_extended evs	string: Base64 encoded binary data.	Bytes. **Note:** The format for each type varies, see the RADIUS RFCs.

"user-group":{}

Optional. This section allows matching a single group to the list of groups that a user

belongs to. This parameter can only be used when `"apply-before-authenticate" == false`. Under this section are the following subitems:

compare":"="

Optional, defaults to `"="`. This item must be either `"="` or `"!="`.

"name":"{{group-name}}"

The group named `"{{group-name}}"` is checked against the user's group memberships.

"return-attrs":[]

This subsection is optional and if not present, no attributes are added to the returned RADIUS packet. The `"return-attrs"` are only added if the policy match is true.

Each element of the `"return-attrs"` array is formatted:

```
{
  "name":"xxxx",
  "value":"xxxx",
  "value-type":"xxxx"
},
```

The descriptions of "name", "value", and "value-type" are defined in the previous **"match":{}** > **"attr":{}** section. One exception is that "value" can be one of the following attributes.

- `"{{group-name}}"` : insert the attribute multiple times once for each group that the user belongs to.
- `"{{group-list}}"` : insert the attribute once with all groups that the user belongs to, separated by commas.

In both exceptions, the `"value-type"` is forced to `"text"`.

"action":"continue"

This item is optional, and defaults to `"continue"`. The `"action"` applies only if the policy match is true. The `"action"` item can be one of three values:

- `"continue"`: Add any `"return-attrs"` and continue on with processing.
- `"reject"`: Add any `"return-attrs"` , send back a RADIUS Access-Reject packet, and end the processing of this RADIUS client (NAS) request.
- `"accept"`: Add any `"return-attrs"` , send back a RADIUS Access-Accept packet, and end the processing of this RADIUS client (NAS) request.

Start the service

You can start the **`IbmRadius.exe`** program either as a Windows service or from the command line.

During the installation, **`IbmRadius.exe`** is configured as a Windows service. It's not initially started because the administrator must set up the `IbmRadiusConfig.json` file first. The service is set to manual start. The service can be manually started. It can be set to automatically start. Errors, warnings and informational messages are sent to the Windows Event log. If the service fails to start, or continues to run, examine the Event Log for possible causes, such as an error in `IbmRadiusConfig.json` file.

The command line invocation of **`IbmRadius.exe`** doesn't use the Event Log, rather it outputs to standard error. It requires the argument `"-run"` and is generally only used for test or debugging purposes. Another useful argument "-attributes" lists all the RADIUS-known RADIUS attributes, their names, value type, and enum values. This argument is useful when you add attributes into the `IbmRadiusConfig.json` file.

Uninstalling the IBM Verify Gateway for RADIUS server

Before you begin

Ensure that the “Event Viewer” isn't running. It can lock the `IbmRadiusMsg.dll` file because it uses the file to display IBM Verify Gateway for RADIUS event messages.

About this task

Procedure

Use the standard Windows **Control Panel** > **Programs** > **Programs and Features** method to remove the server. The Windows service is unregistered and all files except `IbmRadiusConfig.json` and `cacert.pem` are removed. You can remove these files manually or leave them for a subsequent installation.