



思科 ASA REST API 快速入门指南

首次发布：2014 年 12 月 24 日

修订日期：2016 年 12 月 22 日

目录

[概述（第 1 页）](#)

[ASA REST API 请求和响应（第 2 页）](#)

[安装和配置 ASA REST API 代理和客户端（第 3 页）](#)

[文档控制台和导出 API 脚本（第 5 页）](#)

[在 ASA 上启用 REST API 调试（第 6 页）](#)

[ASA REST API 相关的系统日志消息（第 7 页）](#)

[相关文档（第 8 页）](#)

概述

您可以通过多种方式配置和管理单个思科 ASA：

- 命令行界面 (CLI) - 通过连接控制台将控制命令直接发送到 ASA。
- 自适应安全设备管理器 (ASDM) - “内置”管理应用，其图形用户界面可供您配置、管理和监控 ASA。
- 思科安全管理器 - 虽然此图形应用旨在用于由许多安全设备构成的大中型网络，但它也可用来配置、管理和监控单个 ASA。

思科 ASA REST API 的推出为您提供了另一款轻型、易用的选件。这是基于“RESTful”原则的应用编程接口 (API)，可以在运行 API 的任何 ASA 上快速下载和启用这些原则。

在浏览器上安装 REST 客户端之后，您可以联系特定 ASA 的 REST 代理和使用标准 HTTP 方法访问当前配置信息，并发出其他配置参数。



注意

在 ASA 上启用 REST API 后，不会阻止其他安全管理协议的连接。这意味着在您修改 ASA 配置时，使用 CLI、ASDM 或安全管理器的其他用户也可能正在执行相同的操作。



ASA REST API 请求和响应

借助于 ASA REST API，您可以通过具象状态传输 (REST) API 进行编程访问，以管理单个 ASA。该 API 基于 HTTPS 协议和 REST 方法，允许外部客户端对 ASA 资源执行 CRUD（创建、读取、更新、删除）操作。

所有 API 请求均通过 HTTPS 发送到 ASA，并由系统返回响应。

本节概述如何构建请求以及预期响应。

请求结构

可用的请求方法如下：

- GET - 从指定对象检索数据。
- PUT - 将提供的信息添加到指定对象；如果对象不存在，则返回 “404 资源未找到” 错误消息。
- POST - 使用提供的信息创建对象。
- DELETE - 删除指定对象。
- PATCH - 将部分修改应用到指定对象。

响应结构

每个请求均从 ASA 生成一个带有标准报头、响应内容和状态代码的 HTTPS 响应。

响应结构可以是：

- LOCATION - 新创建的资源 ID；仅对于 POST：保留新的资源 ID（作为 URI 表达式）。
- CONTENT-TYPE - 描述响应消息正文的介质类型；描述响应消息正文的表达和语法。

每个响应均包括 HTTP 状态或错误代码。可用的代码属于以下类别：

- 20x - 二百系列代码表示操作成功，包括：
 - 200 OK - 成功请求的标准响应。
 - 201 Created - 已完成请求；已创建新资源。
 - 202 Accepted - 已接受请求，但是未完成处理。
 - 204 No Content - 服务器已成功处理请求；未返回内容。
- 4xx - 四百系列代码表示客户端错误，包括：
 - 400 Bad Request - 无效的查询参数，包括无法识别的参数、缺失的参数或无效值。
 - 404 Not Found - 提供的 URL 与现有资源不匹配。例如，因为资源不可用，HTTP DELETE 可能失败。
 - 405 Method not Allowed - 提出资源上不允许的 HTTP 请求；例如，只读资源上的 POST。
- 5xx - 五百系列代码表示服务器端错误。

一旦出现错误，除了错误代码以外，返回响应还可能包括错误对象（包含有关错误的更多详情）。JSON 错误/警告响应模式如下：

```
[
  { "code"      : "string",
    "details": "string",
    "context": attribute name,
```

```
        "level"    : <Error/Warning/Info>
      },
      ...
    ]
```

其中，对象属性如下：

财产	类型	说明
邮件	词典列表	错误或警告消息列表
code	字符串	错误/警告/信息代码
详细信息	字符串	与 Error/Warning/Info 相对应的详细消息



备注

REST API 调用对 ASA 配置所做的更改不会持久存留到启动配置中；也就是说，只将该更改分配到正在运行的配置中。要保存对启动配置所做的更改，您可以 POST 一个 writemem API 请求；有关详细信息，请参阅《关于 ASA REST API》文档的“写入内存 API”部分。

安装和配置 ASA REST API 代理和客户端

对于物理 ASA，REST API 代理不随 cisco.com 上的其他 ASA 映像一起发布。也就是说，为物理 ASA 提供的映像不包括 REST API 插件包。REST API 软件包必须下载到设备的闪存，并使用 rest-api image 命令安装，然后需要使用 rest-api agent 命令启用 REST API 代理。

对于虚拟 ASA (ASAv)，部署软件包中包括 REST API 映像（在 boot: 分区下提供）。默认情况下，ASAv 未配置为使用 REST API，所以您必须依次使用 rest-api image 命令和 rest-api agent 命令来访问并启用 REST API 代理。



备注

REST API 代理是基于 Java 的应用。Java Runtime Environment (JRE) 捆绑在 REST API 代理软件包中。

以下各节介绍如何在 ASA 上安装和启用 REST API 代理，以及如何在本地主机上添加和配置 REST API 客户端。

下载并安装 REST API 代理

使用 CLI，按照以下步骤在特定 ASA 上下载并安装 ASA REST API 代理：

- 步骤 1

在所需的 ASA 上，发出 copy <package> disk0: 命令，将当前的 ASA REST API 软件包从 cisco.com 下载到 ASA 的闪存中。例如：
copy tftp://10.7.0.80/asa-restapi-111-1fbff-k8.SPA disk0:
- 步骤 2

发出 rest-api image disk0: /<package> 命令以验证和安装软件包。例如：
rest-api image disk0: /asa-restapi-111-1fbff-k8.SPA
- 安装程序将执行兼容性和验证检查，然后安装软件包。ASA 将不会重新启动。

启用并配置 REST API 代理

按照以下步骤在特定 ASA 上启用和配置 ASA REST API 代理：

步骤 1 确保在 ASA 上安装正确的软件映像。

对于 ASA 55nn-X，这是 asa100-12-16-15-smp-k8.bin 或更高版本。对于 ASAv，此映像为 asav100-12-16-15.ova。如果 ASAv 上已经安装 .ova 映像，则可以使用 asa100-12-16-15-smp-k8.bin 更新 VM 映像。

步骤 2 使用 CLI，确保在 ASA 上已启用 HTTP 服务器，并且 API 客户端可以连接到管理接口。例如：

```
http server enable
http 0.0.0.0 0.0.0.0 <management interface nameif>
```

步骤 3 使用 CLI，定义 API 连接的 HTTP 身份验证。例如：

```
aaa authentication http console LOCAL
```

步骤 4 使用 CLI，创建具有读/写权限的本地用户，在这种情况下，权限等级为 15。例如：

```
username <user name> password <password> encrypted privilege 15
```

需要使用权限级别 3 或更高级别才能调用监控请求，而需要使用权限级别 5 或更高级别才能调用 GET 请求，并且，调用 PUT/POST/DELETE 操作需要使用权限级别 15。



注

如果配置了 aaa authorization，REST 代理将要求在 ASA 上定义一个名为 **enable_1** 并且权限级别为 15 的用户。当 REST 代理最初尝试加载和解析 ASA 配置时，以及 ASA 的配置每次发生更改时，REST 代理会使用此用户帐户与 ASA 通信。因此，您可能需要在 AAA 服务器/本地用户数据库中创建一个名为 enable_1 并且权限级别为 15 的用户。

步骤 5 使用 CLI，在 ASA 上为 API 流量创建静态路由。例如：

```
route <management interface nameif> 0.0.0.0 0.0.0.0 <gwip> 1
```

步骤 6 使用 CLI，在 ASA 上启用 ASA REST API 代理。例如：

```
rest-api agent
```

配置 REST API 客户端

按照以下步骤在本地主机浏览器上安装和配置 REST API 客户端：

步骤 1 为浏览器获取并安装 REST API 客户端

对于 Chrome，请从 Google 安装 REST 客户端。对于 Firefox，请安装 RESTClient 插件。不支持 Internet Explorer。

步骤 2 使用浏览器发起以下请求：

```
https:<asa management ip address>/api/objects/networkobjects
```

如果收到非错误响应，说明您已联系到在 ASA 上工作的 REST API 代理。

如有关于代理请求的问题，则可以在 CLI 控制台上启用调试信息的显示，如在 [ASA 上启用 REST API 调试（第 6 页）](#) 所述。

步骤 3 或者，您可以执行 POST 操作，以测试与 ASA 的连接。

例如：

提供基本的授权凭证 (<username><password>) 或身份验证令牌（有关详细信息，请参阅 [令牌身份验证](#)）。

目标请求地址：https://<asa management ipaddress>/api/objects/networkobjects

主体内容类型：application/json

操作的原始主体：

```
{
  "kind": "object#NetworkObj",
  "name": "TestNetworkRangeObj",
  "host": {
    "kind": "IPv4Network",
    "value": "12.12.12.0/24"
  }
}
```

您现在可以使用 ASA REST API 配置和监控 ASA。请参阅 API 文档以获得调用说明和示例。

文档控制台和导出 API 脚本

您还可以使用 REST API 在线文档控制台（称为“文档 UI”），其作为“沙盒”在 *host:port/doc/* 提供，用于直接在 ASA 上了解和尝试 API 调用。

而且，您可以使用文档 UI 上的 **Export Operation** 按钮将显示的方法示例作为 JavaScript、Python 或 Perl 脚本文件保存到本地主机中。然后，您可以将此脚本应用于 ASA，并可以为其他 ASA 和其他网络设备上的应用编辑此脚本。这最初作为教育和引导程序工具。

JavaScript

使用 JavaScript 文件需要安装 node.js，其可从 <http://nodejs.org/> 下载。您可以使用 node.js 执行 JavaScript 文件，该文件通常针对浏览器编写，例如命令行脚本。只需遵循安装说明，然后使用 `node script.js` 运行脚本。

Python

运行 Python 脚本需要安装 Python（可从 <https://www.python.org/> 下载）。安装 Python 后，即可使用 `python script.py username password` 运行脚本。

Perl

使用 Perl 脚本需要安装其他一些组件 - 您需要安装五个组件：Perl 本身和四个 Perl 库：

- Perl 软件包，位于 <http://www.perl.org/>
- Bundle::CPAN，位于 <http://search.cpan.org/~andk/Bundle-CPAN-1.861/CPAN.pm>
- REST::Client，位于 <http://search.cpan.org/~mcrawfor/REST-Client-88/lib/REST/Client.pm>
- MIME::Base64，位于 <http://perldoc.perl.org/MIME/Base64.html>
- JSON，位于 <http://search.cpan.org/~makamaka/JSON-2.90/lib/JSON.pm>

以下是 Macintosh 上引导程序 Perl 的示例

```
$ sudo perl -MCPAN e shell
cpan> install Bundle::CPAN
cpan> install REST::Client
cpan> install MIME::Base64
cpan> install JSON
```

安装相关项后，即可使用 `perl script.pl username password` 运行脚本。

在 ASA 上启用 REST API 调试

如果在 ASA 上配置或连接 REST API 遇到问题，您可以使用以下 CLI 命令在控制台上启用调试消息的显示。使用命令的 **no** 形式可禁用调试消息。

```
debug rest-api [agent | cli | client | daemon | process | token-auth] [error | event]
no debug rest-api
```

语法说明

agent	(可选) 启用 REST API 代理调试信息。
cli	(可选) 为 REST API CLI 后台守护程序与代理的通信启用调试消息。
client	(可选) 为 REST API 客户端与 REST API 代理之间的消息路由启用调试消息。
daemon	(可选) 为 REST API 后台守护程序与代理的通信启用调试消息。
process	(可选) 启用 REST API 代理进程开始/停止调试信息。
token-auth	(可选) REST API 令牌身份验证调试信息。
error	(可选) 使用此关键字将调试消息限定于由 API 记录的错误。
event	(可选) 使用此关键字将调试消息限定于由 API 记录的事件。

使用指南

如不提供特定组件关键字（也就是说，如果只是发出 **debug rest-api** 命令），则为所有组件类型显示调试消息。如不提供 **event** 或 **error** 关键字，则为指定的组件显示事件和错误消息。例如，**debug rest-api daemon event** 将为 API 后台守护程序与代理的通信仅显示事件调试消息。

相关命令

命令	描述
debug http	使用此命令可以查看有关 HTTP 流量的详细信息。

ASA REST API 相关的系统日志消息

本节介绍 ASA REST API 相关的系统日志消息。

342001

错误消息 %ASA-7-342001: REST API Agent started successfully.

说明 在 REST API 客户端可以配置 ASA 之前，必须成功启动 REST API 代理。

建议的操作 无。

342002

错误消息 %ASA-3-342002: REST API Agent failed, reason: *reason*

说明 REST API 代理可能由于各种原因无法启动或者崩溃，并且指定了该原因。

- *reason* - REST API 失败的原因

建议的操作 为解决问题而采取的措施因记录的原因而异。例如，当 Java 进程耗尽内存时，REST API 代理崩溃。如果发生这种情况，则需要重新启动 REST API 代理。如果重新启动未成功，请与思科 TAC 联系确定根本原因并修复。

342003

错误消息 %ASA-3-342003: REST API Agent failure notification received.Agent will be restarted automatically.

说明 已收到 REST API 代理发出的故障通知，并且正尝试重新启动此代理。

建议的操作 无。

342004

错误消息 %ASA-3-342004: Failed to automatically restart the REST API Agent after 5 unsuccessful attempts.Use the 'no rest-api agent' and 'rest-api agent' commands to manually restart the Agent.

说明 多次尝试后，REST API 代理仍未能启动。

建议的操作 请参阅系统日志 %ASA-3-342002（如已记录），以便更好地理解失败原因。尝试通过输入 **no rest-api agent** 命令禁用 REST API 代理，然后再使用 **rest-api agent** 命令重新启用 REST API 代理。

相关文档

使用以下链接找到有关 ASA 及其配置和管理的更多信息：

- 浏览思科 ASA 系列文档: <http://www.cisco.com/go/asadocs>

使用以下链接查看 ASA_v 中不支持的 ASA 功能列表：

- <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/intro-asav.html#pgfId-1156883>

本文档需结合 “相关文档” 一节中列出的文档共同使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴” 一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

© 2014-2015 思科系统公司。版权所有。