Guide de démarrage rapide de Cisco ASA REST API

Dernière modification : 2024-10-10

Guide de démarrage rapide de Cisco ASA REST API

Aperçu

Plusieurs options sont disponibles pour la configuration et la gestion des appareils de sécurité adaptables Cisco individuels :

- Interface de ligne de commande (CLI) – vous envoyez des commandes de contrôle directement à l'appareil de sécurité adaptable Cisco par l'intermédiaire d'une console connectée.
- Le gestionnaire des dispositifs de sécurité adaptatifs (ASDM) est une application de gestion « intégrée » avec une interface interface utilisateur que vous pouvez utiliser pour configurer, gérer et superviser un appareil de sécurité adaptable Cisco.
- Cisco Security Manager – Bien qu'elle soit destinée aux réseaux de taille moyenne à grande comportant de nombreux appareils de sécurité, cette application graphique peut être utilisée pour configurer, gérer et superviser les appareils de sécurité adaptables Cisco individuels.

Avec la sortie de l'API REST de Cisco pour les appareils de sécurité adaptables Cisco, vous disposez maintenant d'une autre option légère et facile à utiliser. Il s'agit d'une application de programmation d'interface (API) basée sur les principes « RESTful » que vous pouvez télécharger et activer rapidement sur n'importe quel appareil de sécurité adaptable Cisco sur lequel l'API est exécutée.

Après avoir installé un client REST dans votre navigateur, vous pouvez contacter l'agent REST de l'appareil concerné et utiliser les méthodes HTTP standard pour accéder aux informations de configuration actuelles et problème des paramètres de configuration supplémentaires.

⚠

Mise en garde Lorsque l'API REST est activée sur un appareil de sécurité adaptable Cisco, les connexions par d'autres protocoles de gestion de la sécurité ne sont pas bloquées. Cela signifie que d'autres personnes qui utilisent l'interface de commande, l'ASDM ou le Security Manager peuvent modifier la configuration de l'appareil de sécurité adaptable Cisco pendant que vous faites de même.

Demandes et réponses de l'API REST ASA

L'API REST ASA vous donne un accéder programmatique à la gestion des interfaces ASA individuelles par le biais d'une API REST (Representational State Transfer) L'API permet aux clients externes d'effectuer des opérations CRUD (Create, Read, Update, Delete) sur les ressources de l'appareil de sécurité adaptable Cisco. Elle est basée sur le protocole HTTPS et la méthodologie REST.

Toutes les requêtes API sont envoyées par HTTPS à l'appareil de sécurité adaptable Cisco, puis une réponse est renvoyée.

Cette section présente un survol de la façon dont les demandes sont structurées et les réponses attendues.

Structure de la demande

Les méthodes de demande disponibles sont les suivantes :

- GET – Extrait les données de l'objet spécifié.
- PUT – Ajoute les informations fournies à l'objet indiqué. Renvoie une erreur 404 indiquant que la ressource est introuvable si l'objet n'existe pas.
- POST – Crée l'objet avec les informations fournies.
- DELETE – Supprime l'objet spécifié.
- PATCH – Applique des modifications partielles à l'objet spécifié.

Structure de la réponse

Chaque demande génère une réponse HTTPS par de l'appareil de sécurité adaptable Cisco avec les en-têtes, le contenu de la réponse et le code d'état standard.

La structure de réponse peut être :

- LOCATION – ID de la ressource nouvellement créée; pour POST uniquement : contient le nouvel ID de la ressource (sous forme de représentation d'URI).
- CONTENT-TYPE – Type de support décrivant le corps du message de réponse; décrit la représentation et la syntaxe du corps du message de la réponse.

Chaque réponse comprend un état HTTP ou un code d'erreur. Les codes disponibles appartiennent aux catégories suivantes :

- `20x` – Un code de la série deux cent indique qu'une opération a réussi, y compris :
  - `200 OK` – Réponse standard pour les demandes ayant réussi.
  - `201 Created` – Demande terminée; nouvelle ressource créée.
  - `202 Accepted` – Demande acceptée, mais traitement incomplet.
  - `204 No Content` – Demande du serveur avec succès; aucun contenu n'est renvoyé.
- `4xx` – Un code de la série quatre cent indique une erreur du côté client, notamment :
  - `400 Bad Request` – Paramètres de la requête non valides, y compris les paramètres non reconnus, les paramètres manquants ou les valeurs non valides.
  - `204 Not Found` – URL fournie qui ne correspond à aucune ressource existante. Par exemple, une demande HTTP DELETE peut échouer, car la ressource n'est pas disponible.
  - `405 Method not Allowed` – Demande HTTP présentée qui n'est pas autorisée pour la ressource; par exemple, une demande POST pour une ressource en lecture seule.
- `5xx` – Un code de la série cinq cent indique une erreur du côté du serveur.

Dans le cas d'une erreur, en plus du code d'erreur, la réponse renvoyée peut inclure un objet erreur contenant plus de détails sur l'erreur. Le schéma de réponse de l'erreur/avertissement JSON est le suivant :

```
[
{ "code" : "string",
"details": "string",
"context": attribute name,
"level" : <Error/Warning/Info>
},
...
]
```

dans lequel les propriétés de l'objet sont :

Propriété	Type	Description
`messages`	Liste des dictionnaires	Liste des messages d'erreur ou d'avertissement
`Code`	Chaîne	Code d'erreur/avertissement/code d'information
`détails`	Chaîne	Message détaillé correspondant à l'erreur/l'avertissement/l'information

Remarque Les modifications à la configuration des appareils de sécurité adaptables Cisco effectuées par les appels d'API REST ne sont pas conservées dans la configuration de démarrage, ce qui veut dire que les modifications sont apportées uniquement à la configuration en cours. Pour enregistrer ces modifications à la configuration de démarrage, vous pouvez utiliser la commande POST pour une demande d'API `writemem`. Pour en savoir plus, consultez l'entrée « Write Memory API » dans la table des matières À propos de l'API REST de l'appareil de sécurité adaptable Cisco.

Installer et configurer l'agent et le client API REST pour l'appareil de sécurité adaptable Cisco

L'agent d'API REST est publié individuellement avec d'autres images pour appareils de sécurité adaptables Cisco sur cisco.com. Pour les appareils de sécurité adaptables Cisco physiques, le paquet API REST doit être téléchargé dans la mémoire flash du périphérique et installé à l'aide de la commande « rest-api image ». L'agent API REST est ensuite activé à l'aide de la commande « rest-api agent ».

Avec un appareil de sécurité adaptable Cisco virtuel (ASAv), l'image de l'API REST doit être téléchargée dans la partition « boot: ». Vous devez ensuite problème la commande « rest-api image » suivie de la commande « rest-api agent » pour accéder à l'agent API REST et l'activer.

Pour en savoir plus sur les exigences et la compatibilité du logiciel et du matériel avec l'API REST, consultez la matrice de compatibilité Cisco ASA.

Vous pouvez télécharger l'ensemble API REST approprié pour votre appareil de sécurité adaptable Cisco ou ASAv de la page software.cisco.com/download/home. Localisez le modèle d'appareil de sécurité adaptable (ASA), puis choisissez le plugiciel Adaptive Security Appliance REST API.

Remarque L'agent API REST est une application basée sur Java. Le Java Runtime Environment (JRE) est inclus dans le paquet de l'agent API REST.

Instructions d'utilisation

Important Vous devez inclure l'en-tête `User-Agent: REST API Agent` dans tous les appels d'API et tous les scripts existants. Utilisez `-H 'User-Agent : REST API Agent'` pour la commande CURL.

En mode multi-contextes, les commandes de l'agent API REST ne sont disponibles que dans le contexte du système.

Taille de configuration maximale prise en charge

L'API Rest de l'appareil de sécurité adaptable Cisco est une application « intégrée » qui s'exécute dans l'appareil de sécurité adaptable Cisco physique et qui, en tant que telle, a une limitation quant à la mémoire qui lui est allouée. La taille maximale de la configuration en cours d'exécution prise en charge a augmenté pendant le cycle de version pour atteindre environ 2 Mo sur les plateformes récentes comme 5555 et 5585.

L'API REST de l'appareil de sécurité adaptable Cisco comprend également des contraintes de mémoire pour les plateformes virtuelles des appareils de sécurité adaptables Cisco. La mémoire totale peut atteindre 1,5 Go sur l'ASAv5, alors qu'elle est de 2 Go sur l'ASAv10. Les limites de l'API Rest sont de 450 Ko et de 500 Ko pour l'ASAv5 et l'ASAv10, respectivement.

Par conséquent, sachez qu'en cours d'exécution, les lourdes configurations peuvent générer des exceptions dans diverses situations nécessitant beaucoup de mémoire, comme un grand nombre de demandes simultanées ou un volume de demandes élevé. Dans ces situations, les appels GET/PUT/POST des API Rest peuvent commencer à échouer et envoyer des messages 500 – Internal Server Error et l'agent d'API Rest redémarrera automatiquement chaque fois.

Les solutions de contournement à ce problème sont soit de passer aux plateformes ASA/FPR ou ASAV dont la mémoire est supérieure, soit de réduire la taille de la configuration en cours.

Taille de configuration maximale prise en charge

L'API Rest de l'appareil de sécurité adaptable Cisco est une application « intégrée » qui s'exécute dans l'appareil de sécurité adaptable Cisco physique et qui, en tant que telle, a une limitation quant à la mémoire qui lui est allouée. La taille maximale de la configuration en cours d'exécution prise en charge a augmenté pendant le cycle de version pour atteindre environ 2 Mo sur les plateformes récentes comme 5555 et 5585.

L'API REST de l'appareil de sécurité adaptable Cisco comprend également des contraintes de mémoire pour les plateformes virtuelles des appareils de sécurité adaptables Cisco. La mémoire totale peut atteindre 1,5 Go sur l'ASAv5, alors qu'elle est de 2 Go sur l'ASAv10. Les limites de l'API Rest sont de 450 Ko et de 500 Ko pour l'ASAv5 et l'ASAv10, respectivement.

Par conséquent, sachez qu'en cours d'exécution, les lourdes configurations peuvent générer des exceptions dans diverses situations nécessitant beaucoup de mémoire, comme un grand nombre de demandes simultanées ou un volume de demandes élevé. Dans ces situations, les appels GET/PUT/POST des API Rest peuvent commencer à échouer et envoyer des messages 500 – Internal Server Error et l'agent d'API Rest redémarrera automatiquement chaque fois.

Les solutions de contournement à ce problème sont soit de passer aux plateformes ASA/FPR ou ASAV dont la mémoire est supérieure, soit de réduire la taille de la configuration en cours.

Télécharger et installer l'agent d'API REST

À l'aide de l'interface de ligne de commande, suivez ces étapes pour télécharger et installer l'agent d'API REST pour l'appareil de sécurité adaptable Cisco sur un appareil de sécurité adaptable Cisco spécifique :

Procédure

Étape 1 Sur l'appareil de sécurité adaptable Cisco souhaité, envoyez la commande de copie `<package> disk0:` pour télécharger dans la mémoire flash de l'appareil le paquet API REST actuel pour l'appareil de sécurité adaptable Cisco actuel. Par exemple :

```
copy tftp://10.7.0.80/asa-restapi-111-lfbff-k8.SPA disk0:
```

Étape 2 Envoyez la commande `rest-api image disk0:/<package>` pour vérifier et installer le paquet.

Par exemple :

```
rest-api image disk0:/asa-restapi-111-lfbff-k8.SPA
```

La version d'installation effectue des vérifications de compatibilité et de validation, puis installe le paquet. L'appareil de sécurité adaptable Cisco ne redémarrera pas.

Activer l'agent de l'API REST

Suivez les étapes suivantes pour activer l'agent d'API REST pour l'appareil de sécurité adaptable Cisco sur un appareil de sécurité adaptable Cisco particulier :

Procédure

Étape 1 Assurez-vous que la bonne image logicielle est installée sur l'appareil de sécurité adaptable Cisco.

Consultez la section sur l'API REST de la matrice de compatibilité des appareils de sécurité adaptables Cisco https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html#pgfId-131643 pour déterminer quelle image Appareils de sécurité adaptables Cisco est requise.

Étape 2 À l'aide de l'interface de ligne de commande, assurez-vous que le serveur HTTP est activé sur l'appareil de sécurité adaptable Cisco et que les clients de l'API peuvent se connecter à l'interface de gestion. Par exemple :

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

Étape 3 À l'aide de l'interface de ligne de commande, définissez l'authentification HTTP pour les connexions par API. Par exemple :

```
aaa authentication http console LOCAL
```

Étape 4 À l'aide de l'interface de ligne de commande, créez une voie de route statique sur l'appareil de sécurité adaptable Cisco pour le trafic de l'API. Par exemple :

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

Étape 5 À l'aide de l'interface de ligne de commande, activez l'agent API REST pour l'appareil de sécurité adaptable Cisco sur l'appareil de sécurité adaptable Cisco. Par exemple :

```
rest-api agent
```

Authentification de l'API REST

Il existe deux façons de s'authentifier, soit l'authentification HTTP de base qui envoie un nom utilisateur et un mot de mot de passe dans chacune des demandes, ou l'authentification par jeton avec transport sécurisé HTTPS qui transmet un jeton créé précédemment avec chacune des demandes. Dans tous les cas, l'authentification sera effectuée pour chacune des demandes. Consultez la section « Token_Authentication_API » dans le guide *À propos de l'API REST pour l'appareil de sécurité adaptable Cisco v7.14(x)* pour en savoir plus sur l'authentification par jeton.

Remarque L'utilisation des certificats émis par l'autorité de certification (CA) est recommandée sur les appareils de sécurité adaptables Cisco afin que les clients de l'API REST puissent valider les certificats du serveur pour les appareils de sécurité adaptables Cisco lors de l'établissement des connexions SSL.

Autorisation de commande

Si l'autorisation de commande est configurée pour utiliser un serveur AAA externe (par exemple, `aaa authorization command <TACACS+_server>`), un utilisateur nommé **enable_1** doit exister sur ce serveur et avoir tous les privilèges de commande.

Si l'autorisation de commande est configurée pour utiliser la base de données LOCALE de l'ASA (`aaa authorization command LOCAL`), tous les utilisateurs de l'API REST doivent être inscrits dans la base de données LOCAL avec des niveaux de privilèges appropriés selon leurs rôles :

- Un niveau de privilège 3 ou supérieur est requis pour appeler des demandes de supervision.
- Un niveau de privilège 5 ou supérieur est requis pour appeler les demandes GET.
- Un niveau de privilège 15 est nécessaire pour appeler les opérations PUT/POST/DELETE.

Configurez votre client API REST

Suivez les étapes suivantes pour installer et configurer un client API REST sur le navigateur de votre hôte local :

Procédure

Étape 1 Procurez-vous et installez un client API REST pour votre navigateur.

Pour Chrome, installez le client REST de Google. Pour Firefox, installez le module complémentaire RESTClient. Internet Explorer n'est pas pris en charge.

Étape 2 Lancez la demande suivante à l'aide de votre navigateur :

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

Si vous recevez une réponse sans erreur, vous avez atteint l'agent API REST fonctionnant sur l'appareil de sécurité adaptable Cisco.

Si vous éprouvez des problèmes avec la demande de l'agent, vous pouvez activer l'affichage des informations de débogage sur la console de l'interface de ligne de commande, comme cela est décrit dans la section Activer la fonction de débogage de l'API REST sur l'appareil de sécurité adaptable Cisco.

Étape 3 Vous pouvez également tesert votre connexion à l'appareil de sécurité adaptable Cisco en effectuant une opération POST.

Par exemple :

Fournissez les identifiants de base *(<username><password>)* ou un jeton d'authentification (consultez la section Authentification par jeton pour en savoir plus).

Adresse de la demande cible : `https://<asa management ipaddress>/api/objects/networkobjects`

Type de contenu du corps : `application/json`

Corps brut de l'opération :

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

Vous pouvez maintenant utiliser l'API REST de l'appareil de sécurité adaptable Cisco pour configurer et superviser l'appareil de sécurité adaptable Cisco. Consultez la documentation sur l'API pour obtenir des descriptions d'appels et des exemples.

À propos de la restauration complète d'une configuration de sauvegarde

La restauration d'une configuration de sauvegarde complète sur l'appareil de sécurité adaptable Cisco à l'aide de l'API REST rechargera l'appareil de sécurité adaptable Cisco. Pour éviter cela, utilisez la commande suivante pour restaurer une configuration de sauvegarde :

```
{
"commands":["copy /noconfirm disk0:/<filename> running-config"]
}
```

Dans laquelle *<filename>* est la sauvegarde (back.cfg) ou quel qu'autre nom que vous avez utilisé lors de la sauvegarde de la configuration.

Console de documentation et exportation des scripts d'API

Vous pouvez également utiliser la console de documentation en ligne de l'API REST (appelée « interface utilisateur de la documentation »), disponible sur *host:port/doc/* comme « bac à sable » pour en apprendre davantage sur les appels d'API directement sur l'appareil de sécurité adaptable Cisco et les essayer.

En outre, vous pouvez utiliser le bouton **Export Operation** dans l'interface utilisateur de la documentation pour enregistrer l'exemple de méthode affiché en tant que fichier script javascript, Python ou Perl sur votre hôte local. Vous pouvez ensuite appliquer ce script à votre appareil de sécurité adaptable Cisco et le modifier pour l'utiliser sur d'autres ASA et d'autres périphériques réseau. Il a surtout été conçu comme un outil pédagogique et de démarrage.

JavaScript

L'utilisation d'un fichier javascript nécessite l'installation de `node.js`, qui se trouve à l'adresse `http://nodejs.org/. À l'aide de node.js`, vous pouvez exécuter un fichier javascript généralement écrit pour un navigateur, comme un script pour ligne de commande. Suivez simplement les instructions d'installation, puis exécutez votre script avec le script de `node script.js`.

Python

Les scripts Python nécessitent l'installation de Python, disponible sur le site `https://www.python.org/`. Une fois que vous avez installé Python, vous pouvez exécuter votre script avec `python script.py nom d'utilisateur mot de passe`.

Perl

L'utilisation des scripts Perl nécessite une configuration supplémentaire. Vous aurez besoin de cinq composants, soit Perl lui-même et quatre bibliothèques Perl :

- Perl package disponible à l'adresse `http://www.perl.org/`
- Bundle::CPAN disponible à l'adresse `http://search.cpan.org/~andk/Bundle-CPAN-1.861/CPAN.pm`
- REST::Client disponible à l'adresse `http://search.cpan.org/%7Emcrawfor/REST-Client-88/lib/REST/Client.pm`
- MIME::Base64 disponible à l'adresse `http://perldoc.perl.org/MIME/Base64.html`
- JSON disponible à l'adresse `http://search.cpan.org/~makamaka/JSON-2.90/lib/JSON.pm`

Voici un exemple de démarrage de Perl sur un Macintosh :

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

Après avoir installé les dépendances, vous pouvez exécuter votre script en utilisant le script `perl script.pl nom d'utilisateur mot de mot de passe`.

Activer la fonction de débogage de l'API REST sur l'appareil de sécurité adaptable Cisco

Si vous éprouvez des problèmes lors de la configuration de l'API REST sur l'appareil de sécurité adaptable Cisco ou de la connexion à l'API, vous pouvez utiliser la commande CLI suivante pour activer l'affichage des messages de débogage sur votre console. Utilisez la forme sans forme de la commande pour désactiver les messages de débogage.

debug rest-api [**agent** | **cli** | **client** | **daemon** | **process** | **oken-auth**] [**error** | **event**]

no debug rest-api

Description de la syntaxe

agent	(Facultatif) Activez les informations de débogage de l'agent API REST.
cli	(Facultatif) Activez les messages de débogage pour les communications entre le démon de l'interface de commande en ligne de l'API REST.
client	(Facultatif) Activez les informations de débogage pour le routage des messages entre le client API REST et l'agent API REST.
daemon	(Facultatif) Activez les messages de débogage pour les communications entre le démon API REST et l'agent.
process	(Facultatif) Activez les informations de débogage pour le démarrage et l'arrêt du processus de l'agent API REST.
token-auth	(Facultatif) Informations de débogage pour l'authentification par jeton de l'API REST.
error	(Facultatif) Utilisez ce mot-clé pour limiter les messages de débogage aux erreurs enregistrées par l'API.
event	(Facultatif) Utilisez ce mot-clé pour limiter les messages de débogage aux événements enregistrés par l'API.

Instructions d'utilisation

Si vous ne fournissez pas de mot-clé pour un composant particulier (c'est-à-dire si vous donnez simplement la commande **debug rest-api**), des messages de débogage s'afficheront pour tous les types de composants. Si vous ne fournissez pas de mot-clé **event** ou **error**, les messages d'événement et d'erreur s'afficheront pour le composant précisé. Par exemple, **debug rest-api daemon event** affichera uniquement les messages de débogage d'événement pour les communications entre le démon de l'API et l'agent.

Commandes associées

Commande	Description
debug http	Utilisez cette commande pour afficher des informations détaillées sur le trafic HTTP.

Messages du journal système relatifs à l'API REST pour les appareils de sécurité adaptables Cisco

Les messages du journal système liés à l'API REST pour les appareils de sécurité adaptables Cisco sont décrits dans cette section.

Documentation associée

Utilisez le lien suivant pour obtenir plus de renseignements sur l'appareil de sécurité adaptable Cisco, sa configuration et sa gestion :

- *Orientation dans la documentation sur la gamme Cisco ASA :* http://www.cisco.com/go/asadocsxm-replace_text%20List%20Item

Utilisez le lien suivant pour afficher la liste des fonctionnalités de l'appareil de sécurité adaptable Cisco non prises en charge par ASAv :

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

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.