

Comment est-ce que je surveille les santés de l'ESA ?

Contenu

[Introduction](#)

[Comment est-ce que je surveille les santés de l'ESA ?](#)

Introduction

Ce document décrit comment vous pouvez surveiller des services sur l'appliance de sécurité du courrier électronique (ESA).

Comment est-ce que je surveille les santés de l'ESA ?

L'ESA a plusieurs services réseau externe-accessibles qui peuvent être utilisés pour surveiller les santés et le statut du système.

1. L'ESA répondra aux datagrammes de REQUÊTE D'ÉCHO d'ICMP (généralement appelés les messages de « ping »). Un test simple de « ping » peut déterminer l'accessibilité par IP de base de l'appliance et s'il a l'alimentation et fonctionne normalement au plus inférieur du système d'exploitation. Toutes les interfaces IP configurées répondront aux paquets d'ICMP.
2. L'ESA peut être surveillé utilisant des outils de stations de gestion SNMP et de surveillance SNMP. Le MIB SNMP pris en charge est le MIB-II IETF-normalisé. Ceci peut être utilisé pour voir des statistiques inférieures d'IP-couche et de couche transport, telles que des datagrammes et des octets dans et hors du système. La gestion SNMP doit être activée avec la commande CLI de « **snmpconfig** ». Seulement une interface peut être activée à la fois recevoir des requêtes SNMP (bien que la base de données MIB-II couvre le système entier). En outre, si vous utilisez SNMP v1/v2c, vous devez spécifier le réseau que vos requêtes SNMP proviendront. L'ESA peut envoyer un déroutement SNMP de coldStart à une station simple de Gestion, si configuré utilisant la commande CLI de « **snmpconfig** ». Ceci peut être utilisé pour détecter des réinitialisations de système aussi bien que des reprises d'agent SNMP. Cisco fournit un MIB de « entreprise » aussi bien qu'un fichier de « structure de gestion des informations » (SMI) pour l'ESA.
3. Si configuré, l'ESA offrira des services de SMTP, de FTP, de SSH, de HTTP, et HTTPS sur n'importe quelle interface. Ces services peuvent être individuellement activés ou désactivés. L'ESA prend en charge également l'accès décrypté de TELNET, bien que ceci soit fortement découragé. La surveillance des outils peut se connecter à un ou plusieurs de ces services sur un ou plusieurs interfaces pour vérifier que les services sont exécutants et renvoyants la bannière correcte. La configuration des services autre que le SMTP est manipulée utilisant la commande CLI de « **interfaceconfig** » ; la configuration des services de SMTP est manipulée

avec la commande CLI de « **listenerconfig** ».

4. Dans le XML d'AsyncOS les statistiques et les informations d'état sont disponibles par l'intermédiaire des méthodes d'accès de HTTP ou HTTPS. Ces des statistiques XML peuvent être recueillies par une application de contrôle ou un outil de ligne de commande tel que la « **boucle** ». Par exemple, parce que un ESA avec le mot de passe administratif "cisco123," les commandes suivantes de « **boucle** » récupéreront un grand choix d'informations :

```
curl -k https://esa.example.com/xml/status -u admin:cisco123
```

```
curl -k https://esa.example.com/xml/dnsstatus -u admin:cisco123
```

```
curl -k https://esa.example.com/xml/topin -u admin:cisco123
```

```
curl -k https://esa.example.com/xml/tophosts -u admin:cisco123
```

```
curl -k https://esa.example.com/xml/hoststatus -u admin:cisco123 -F hostname=example.com
```

Pour plus d'informations sur l'état du système SNMP, allez au GUI ESA et choisissez l'**aide et le support > aide en ligne**.