

el vESA no puede descargar y aplicar las actualizaciones para Antispam o el antivirus

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[el vESA no puede descargar y aplicar las actualizaciones para Antispam o el antivirus](#)

[Fije el dispositivo para utilizar el host dinámico correcto URL](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cuando un dispositivo de seguridad virtual del correo electrónico (vESA) no descarga y aplica las actualizaciones para el motor del antispam de Cisco (CASO) o el antivirus de Sophos y/o del McAfee, aunque el dispositivo virtual se autoriza correctamente.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad del correo electrónico (ESA)
- vESA, dispositivo de seguridad del Web virtual (vWSA), dispositivo virtual de la Administración de seguridad (vSMA)
- AsyncOS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- vESA, esos funcionamientos AsyncOS 8.0.0 y posterior
- vWSA, esos funcionamientos AsyncOS 7.7.5 y posterior
- vSMA, esos funcionamientos AsyncOS 9.0.0 y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

el vESA no puede descargar y aplicar las actualizaciones para Antispam o el antivirus

Cuando usted pone al día el antispam o el antivirus, los procesos no pueden alcanzar hacia fuera y poner al día el motor o los rulesets del servicio, incluso si usted ingresa el comando de la fuerza de la actualización.

Uno de estos comandos se pudo haber ingresado directamente del CLI en el vESA:

```
> antispamupdate ironport
>antispamupdate ironport force
>antivirusupdate force
>updatenow force
```

Cuando usted ejecuta los **updater_logs de la cola**, los errores considerados son similares a éstos:

```
Mon Oct 21 17:48:43 2013 Info: Dynamic manifest fetch failure: Received invalid
update manifest response
```

Esto indica que el host dinámico URL asociado a la configuración de la actualización no puede alcanzar el updater apropiado evidente correctamente. El host dinámico URL se fija dentro del comando del **updateconfig**. El submandato, **dynamichost**, es comando oculto dentro del **updateconfig**, según lo resaltado aquí:

```
myesa.local> updateconfig
Service (images): Update URL:
-----
Feature Key updates http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
IMS Secondary Service rules Cisco IronPort Servers
Service (list): Update URL:
-----
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Service (list): Update URL:
-----
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
[ ]> dynamichost
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]>
```

Fije el dispositivo para utilizar el host dinámico correcto URL

Hay dos diverso host dinámico URL que se utilicen para los clientes basados en cómo son asociados con Cisco:

- update-manifests.sco.cisco.com:443
- Uso: VESA del cliente, vWSA, vSMA

Nota: Los dispositivos de hardware (C1x0, C3x0, C6x0, y X10x0) deben utilizar SOLAMENTE el host dinámico URL ofupdate-manifests.ironport.com:443. Si hay una configuración de clúster con el ESA y el vESA, el **updateconfig** debe ser configurado en el nivel de equipo y después confirmar que el **dynamichost** está fijado por consiguiente.

- stage-stg-updates.ironport.com:443
- Uso: Friendlies, virtual beta y dispositivos de hardware

Nota: Los clientes deben utilizar solamente el servidor de actualización URL del estacionamiento si han accedido a preprovisioning con Cisco para el uso beta solamente. Si usted no tiene una licencia válida solicitada el uso beta, su dispositivo no recibirá las actualizaciones de los servidores de actualización del estacionamiento.

Como continuación del **updateconfig** y del submandato del **dynamichost**, ingrese el host dinámico URL según lo necesitado, vuelta al prompt principal CLI, y confíe los cambios:

```
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]> stage-stg-updates.ironport.com:443
[]> <<<HIT RETURN TO GO BACK TO THE MAIN CLI PROMPT>>>
```

```
myesa.local> commit
```

Verificación

Para verificar que el dispositivo ahora alcance hacia fuera al host dinámico apropiado URL y a las actualizaciones sea acertado, complete estos pasos:

1. Aumente los **updater_logs** para hacer el debug de. Currently configured logs:> logconfig

```
Log Name Log Type Retrieval Interval
-----
1. antispam Anti-Spam Logs Manual Download None
[SNIP FOR BREVITY]
28. updater_logs Updater Logs Manual Download None
29. upgrade_logs Upgrade Logs Manual Download None
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> edit
Enter the number of the log you wish to edit.
[]> 28 [NOTE, log # will be different on a per/appliance basis]
Please enter the name for the log:
[updater_logs]>
Log level:
```

```
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
[SNIP FOR BREVITY]
```

```
myesa_2.local> commit
```

2. Funcione con una actualización de la fuerza en el antispam (**fuerza del antispamupdate**) o el antivirus (**fuerza del antivirusupdate**). myesa.local> antivirusupdate force

```
Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
```

3. Finalmente, los **updater_logs de la cola** y se aseguran de que el dispositivo pueda alcanzar el **dynamichost** según lo indicado: Mon Oct 21 18:19:12 2013 Debug: Acquiring dynamic manifest from stage-stg-updates.ironport.com:443

Troubleshooting

Complete estos pasos para resolver problemas cualquier problema:

1. Asegúrese de que el **updateconfig** predeterminado esté utilizado. Si el vESA o el host está detrás de un Firewall, asegúrese de que las [actualizaciones con un servidor estático](#) sean funcionando.
2. Asegúrese de que usted pueda **telnet al host dinámico URL** según lo elegido: > telnet
Please select which interface you want to telnet from.
1. Auto
2. Management (172.16.6.165/24: myesa_2.local)
3. new_data (192.168.1.10/24: myesa.local_data1)
[1]>
Enter the remote hostname or IP address.
[> [stage-stg-updates.ironport.com](#)
Enter the remote port.
[25]> 443
Trying 208.90.58.24...
Connected to stage-stg-updates.ironport.com.
Escape character is '^]'.
^] ["CTRL +]"
telnet> quit
Connection closed.

Información Relacionada

- [Actualizaciones o actualizaciones contentas del dispositivo de seguridad con un servidor estático](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)