vESA non è in grado di scaricare e applicare aggiornamenti per Antispam o Antivirus

Sommario

Introduzione

In questo documento viene descritto quando una appliance virtuale di sicurezza e-mail (vESA) non scarica e non applica aggiornamenti per il motore antispam Cisco (CASE) o per l'antivirus Sophos e/o McAfee, anche se la licenza dell'appliance virtuale è corretta.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Email Security Appliance (ESA)
- vESA, virtual Web Security Appliance (vWSA), virtual Security Management Appliance (vSMA)
- AsyncOS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- vESA, con AsyncOS 8.0.0 e versioni successive
- vWSA, con AsyncOS 7.7.5 e versioni successive
- vSMA, con AsyncOS 9.0.0 e versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

vESA non è in grado di scaricare e applicare aggiornamenti per Antispam o Antivirus

Quando si aggiorna la protezione antispam o antivirus, i processi non sono in grado di raggiungere e aggiornare il motore del servizio o i set di regole, anche se si immette il comando **update force**.

Uno di questi comandi potrebbe essere stato immesso direttamente dalla CLI sull'ESA vSA:

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

Quando si esegue **tail updater_logs**, gli errori rilevati sono simili ai seguenti:

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

Ciò indica che l'URL dell'host dinamico associato alla configurazione di aggiornamento non è in grado di raggiungere correttamente il manifesto dell'utilità di aggiornamento appropriato. L'URL dell'host dinamico viene impostato nel comando **updateconfig**. Il sottocomando **dynamichost** è un comando nascosto in **updateconfig**, come evidenziato di seguito:

```
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]>
```

Impostazione dell'accessorio per l'utilizzo dell'URL dell'host dinamico corretto

I clienti possono usare due diversi URL host dinamici a seconda di come vengono associati tramite Cisco:

1. update-manifests.sco.cisco.com:443 Utilizzo: Cliente vESA, vWSA, vSMA
2. stage-stg-updates.ironport.com:443 Utilizzo: Amici, dispositivi Beta virtuali e hardware

Nota: Gli accessori hardware (C1x0, C3x0, C6x0 e X10x0) devono utilizzare SOLO l'URL dell'host dinamico *update-manifests.ironport.com:443*. Se è presente una configurazione cluster con ESA e vESA, è necessario configurare **updateconfig** a livello di computer e quindi verificare che **dynamichost** sia impostato di conseguenza.

Nota: I clienti devono utilizzare gli URL del server di aggiornamento di gestione temporanea solo se hanno ottenuto l'accesso al preprovisioning tramite Cisco solo per l'utilizzo Beta. Se non si dispone di una licenza valida per l'utilizzo Beta, l'accessorio non riceverà aggiornamenti dai server di aggiornamento di gestione temporanea.

Come continuazione di **updateconfig** e del sottocomando **dynamichost**, immettere l'URL dell'host dinamico in base alle esigenze, tornare al prompt della CLI principale e eseguire il commit delle modifiche:

```
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
```

Verifica

Per verificare che l'accessorio raggiunga l'URL dell'host dinamico corretto e che gli aggiornamenti siano stati eseguiti correttamente, attenersi alla seguente procedura:

1. Aumentare il valore di **updater_logs** per eseguire il **debug**.
```
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. Eseguire un aggiornamento forzato su antispam (**antispamupdate force**) o antivirus (**antivirusupdate force**).
```
myesa.local> antivirusupdate force

Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
```
3. Infine, eseguire il comando **tail updater_logs** e verificare che l'accessorio sia in grado di raggiungere il dynamichost come indicato:
```
Mon Oct 21 18:19:12 2013 Debug: Acquiring dynamic manifest from stage-stg-
updates.ironport.com:443
```

Risoluzione dei problemi

Per risolvere i problemi, completare i seguenti passaggi:

1. Assicurarsi che venga utilizzata la **configurazione** predefinita di **updateconfig**. Se vESA o l'host è protetto da un firewall, verificare che gli aggiornamenti con un server statico siano in uso.
2. Verificare che sia possibile eseguire il **telnet** all'URL dell'host dinamico come scelto:
```
> 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.
```

Informazioni correlate

- Aggiornamento di Content Security Appliance con un server statico
- Documentazione e supporto tecnico – Cisco Systems