Risoluzione dei problemi relativi al messaggio di avviso - Aggiornamento non riuscito

Sommario

Introduzione

In questo documento viene descritto come identificare, risolvere i problemi e risolvere gli avvisi relativi agli errori di aggiornamento.

Contributo di Dennis McCabe Jr, Technical Leader di Cisco.

Prerequisiti

Requisiti

Cisco raccomanda una conoscenza di base di Cisco Secure Email Gateway o Cisco Secure Email Cloud Gateway.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Premesse

Viene inviato un avviso quando un aggiornamento non è riuscito 3 o più volte per uno dei motori di scansione. Di seguito è riportato un esempio di errore di Greymail nel completare un aggiornamento.

```
The graymail application tried and failed 3 times to successfully complete an update.
```

Identificazione

Per identificare questo problema, è innanzitutto necessario confermare che si stanno ancora ricevendo avvisi relativi a errori di aggiornamento. Per questo motivo, è possibile eseguire il comando display alert dalla CLI.

<#root>

```
(esa.example.local) (SERVICE)>
```

displayalerts

```
Date and Time Stamp Description
--------------------------------------------------------------------------------
22 Nov 2024 12:00:00 +0300 The graymail application tried and failed 3 times to successfully complete a
```

outage.

Da qui, è possibile rivedere i file updater_logs dalla CLI per verificare quando si è verificato l'ultimo errore.

<#root>

```
esa.example.local (SERVICE)>
```

grep -i "update failed" updater_logs

```
Fri Nov 22 12:00:00 2024 Warning: graymail update failed
```

Se l'ultimo errore si è verificato qualche tempo fa, è probabile che sia dovuto a una latenza di rete lieve e che l'avviso possa essere ignorato senza problemi.

Per maggiore sicurezza, possiamo finalmente eseguire il comando enginestatus all dalla CLI e confermare che i motori e le regole siano stati aggiornati correttamente. Tenete presente che i motori vengono aggiornati meno spesso rispetto alle regole. Quindi, mentre è possibile vedere

regole aggiornate negli ultimi 5-10 minuti, potrebbe essere un paio di giorni o settimane dall'ultimo aggiornamento del motore.

<#root>

```
(Machine esa.example.local)>
```

enginestatus all

```
Component      Version      Last Updated      File      Version
CASE Core Files 3.13.2-045 14 Nov 2024 04:06 (GMT +00:00) 1731414068326236
CASE Utilities 3.13.2-045 14 Nov 2024 04:06 (GMT +00:00) 1731414072027229
Structural Rules 3.13.2-20241121_201008 21 Nov 2024 23:30 (GMT +00:00) 1732231660607257
Web Reputation DB 20241016_150447 14 Nov 2024 04:06 (GMT +00:00) 1729091106299038
Web Reputation DB Update 20241016_150447-20241016_150447 14 Nov 2024 04:06 (GMT +00:00) 172909110643616
Content Rules 20241122_021309 22 Nov 2024 02:15 (GMT +00:00) 1732241625451653
Content Rules Update 20241122_022837 22 Nov 2024 02:30 (GMT +00:00) 1732242536816053
Bayes DB 20241122_004336-20241122_013648 22 Nov 2024 01:40 (GMT +00:00) 1732239454073553

SOPHOS Status: UP CPU: 0.0% RAM: 396M
Component Version Last Updated File Version
Sophos Anti-Virus Engine 3.2.07.392.0_6.12 14 Nov 2024 04:06 (GMT +00:00) 1729232666
Sophos IDE Rules 2024112103 21 Nov 2024 22:55 (GMT +00:00) 1732228972

GRAYMAIL Status: UP CPU: 0.0% RAM: 280M
Component Version Last Updated File Version
Graymail Engine 01.430.00 Never updated 143000
Graymail Rules 01.431.37#45 22 Nov 2024 02:25 (GMT +00:00) 1709881322
Graymail Tools 8.0-006 Never updated 1110080006

MCAFEE Status: UP CPU: 0.0% RAM: 670M
Component Version Last Updated File Version
McAfee Engine 6700 Never updated 6700
McAfee DATs 11263 21 Nov 2024 11:29 (GMT +00:00) 1732187479

AMP Status: UP CPU: 0.0% RAM: 163M
Component Version Last Updated File Version
AMP Client Settings 15.0.0-006 14 Nov 2024 04:06 (GMT +00:00) 100110
AMP Client Engine 1.0 Never updated 10
```

Risoluzione

Connettività di rete

Se i problemi persistono, è possibile adottare alcune misure per risolverli ulteriormente.

1. Verificare l'indice del firewall nella versione AsyncOS corrispondente alla build ed eseguire alcuni test di connettività di rete di base. Qui abbiamo alcuni test telnet che mostrano sessioni Connected riuscite, che è quello che stiamo cercando.
    1. Fate clic qui per selezionare una delle opzioni disponibili per AsyncOS 16.0
2. Se uno o più di questi test hanno esito negativo, è necessario verificare che la rete abbia

consentito il traffico in uscita e riprovare.

```
<#root>
(Machine esa.example.local)>
telnet updates.ironport.com 80


Trying 23.62.46.116...
Connected
 to a23-62-46-116.deploy.static.akamaitechnologies.com.
(Machine esa.example.local)>
telnet downloads.ironport.com 80


Trying 96.16.55.20...
Connected
 to a96-16-55-20.deploy.static.akamaitechnologies.com.
(Machine esa.example.local)>
telnet update-manifests.ironport.com 443


Trying 208.90.58.5...
Connected
 to update-manifests.ironport.com.
(Machine esa.example.local)>
telnet update-manifests.sco.cisco.com 443


Trying 208.90.58.6...
Connected
 to update-manifests.sco.cisco.com.
```

Utilizzo server manifesto

1. Si noti che update-manifests.ironport.com viene utilizzato per le appliance fisiche, mentre update-manifests.cisco.com viene utilizzato dalle macchine virtuali. Per verificare che l'host utilizzato sia quello corretto, è possibile eseguire il comando updateconfig seguito da dynamichost. Se non è corretto, assicurarsi di correggere hostname:port, quindi eseguire il commit e salvare le modifiche.

```
<#root>

(Cluster esa.lab)>

updateconfig



Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLUSTERSET - Set how updates are configured in a cluster
- CLUSTERSHOW - Display how updates are configured in a cluster
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>

dynamichost



This command is restricted to "machine" mode. Would you like to switch to "machine" mode? [Y]>

Choose a machine.
1. esa1.lab.local
2. esa2.lab.local
[1]>

Enter new manifest hostname:port
[

update-manifests.sco.cisco.com:443

]>
```

Se nonostante tutti i passaggi descritti si verificano ancora errori di aggiornamento, procedere con l'apertura di una richiesta TAC di Cisco, in modo da ricevere assistenza.

Informazioni correlate

- Guide per l'utente finale di Cisco Secure Email Cloud Gateway
- Guide per l'utente finale di Cisco Secure Email Gateway
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).