

Problembehandlung bei Warnmeldung - Aktualisierung fehlgeschlagen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Identifizieren](#)

[Auflösen](#)

[Netzwerkonnktivität](#)

[Verwendung des Manifestservers](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Identifizierung, Fehlerbehebung und Behebung von Warnungen bei Update-Fehlern beschrieben.

Beitrag von Dennis McCabe Jr, Cisco Technical Leader.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit dem Cisco Secure Email Gateway oder dem Cisco Secure Email Cloud Gateway vertraut sind.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Eine Warnung wird gesendet, wenn eine Aktualisierung für eines der Scan-Engines drei- oder mehrmals fehlgeschlagen ist. Hier ist ein Beispiel, wie Graymail ein Update nicht erfolgreich abschließen konnte.

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

Identifizieren

Um dieses Problem zu identifizieren, können wir zunächst bestätigen, dass wir immer noch Warnungen über fehlgeschlagene Updates erhalten. Zu diesem Zweck können Sie den Befehl `displayalerts` über die CLI ausführen.

```
<#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.
```

Anschließend können wir die `Updater_logs` aus der CLI überprüfen, um zu bestätigen, wann der letzte Fehler aufgetreten ist.

```
<#root>
```

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

```
grep -i "update failed" updater_logs
```

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

Wenn der letzte Fehler schon eine Weile her ist, dann ist es wahrscheinlich, dass er durch ein bisschen Netzwerklatenz verursacht wurde, und die Warnung kann sicher ignoriert werden.

Zur weiteren Beruhigung können wir endlich den Befehl `enginestatus all` aus der CLI ausführen und bestätigen, dass die Engines und Regeln tatsächlich erfolgreich aktualisiert werden. Beachten Sie, dass die Engines seltener aktualisiert werden als die Regeln. Während Sie also die Regeln

sehen, die zuletzt innerhalb der letzten 5-10 Minuten aktualisiert wurden, kann es ein paar Tage oder Wochen seit dem letzten Engine-Update dauern.

```
<#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
```

Auflösen

Netzwerkonnektivität

Wenn die Fehler weiterhin auftreten, gibt es einige Dinge, die wir tun können, um weitere Fehler zu beheben.

1. Überprüfen Sie den Firewall-Index in der entsprechenden AsyncOS-Version, die mit Ihrem Build übereinstimmt, und führen Sie einige grundlegende Netzwerkverbindungstests durch. Hier sehen Sie einige Telnet-Tests, die erfolgreiche Connected Sessions aufzeigen. Das ist genau das, wonach wir suchen.

1. [Klicken Sie hier](#), um eine verfügbare Version für AsyncOS 16.0 anzuzeigen.
2. Wenn einer oder mehrere dieser Tests fehlschlagen, müssen Sie sicherstellen, dass Ihr Netzwerk diesen ausgehenden Datenverkehr zugelassen hat, und den Vorgang wiederholen.

```
<#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.
```

Verwendung des Manifestservers

1. Beachten Sie, dass update-manifests.ironport.com für physische Appliances verwendet wird, während update-manifests.sco.cisco.com von virtuellen Systemen verwendet wird. Um

sicherzustellen, dass der richtige Host verwendet wird, können Sie den Befehl `updateconfig` gefolgt von `dynamichost` ausführen. Wenn sie falsch ist, korrigieren Sie den Hostnamen:port, und bestätigen Sie die Änderungen, und speichern Sie sie.

```
<#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
```

```
]>
```

Wenn Sie die einzelnen Schritte durchgeführt haben und weiterhin Fehler bei Updates feststellen, öffnen Sie ein Cisco TAC-Ticket, und wir können Sie unterstützen.

## Zugehörige Informationen

- [Cisco Secure Email Cloud Gateway - Benutzerhandbücher](#)
- [Cisco Secure Email Gateway - Benutzerhandbücher](#)
- [Technischer Support und Downloads von Cisco](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.