

경고 메시지 트러블슈팅 - 업데이트 실패

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[식별](#)

[해결 중](#)

[네트워크 연결](#)

[매니페스트 서버 사용](#)

[관련 정보](#)

소개

이 문서에서는 업데이트 실패와 관련된 알림 식별, 문제 해결 및 해결에 대해 설명합니다.

기고자: Dennis McCabe Jr, Cisco 기술 리더.

사전 요구 사항

요구 사항

Cisco는 Cisco Secure Email Gateway 또는 Cisco Secure Email Cloud Gateway에 대해 기본적으로 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

검사 엔진 중 하나에 대해 업데이트가 3회 이상 실패하면 알림이 전송됩니다. 다음은 그레이메일이 성공적으로 업데이트를 완료하지 못한 예입니다.

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

식별

이 문제를 파악하기 위해 먼저 업데이트 실패와 관련된 알림을 계속 받고 있음을 확인할 수 있습니다. 이를 위해 CLI에서 `displayalerts` 명령을 실행할 수 있습니다.

```
<#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.
```

그런 다음 CLI에서 `updater_logs`를 검토하여 마지막 장애가 발생한 시간을 확인할 수 있습니다.

```
<#root>
```

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

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

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

마지막 장애가 얼마 전이었다면 약간의 네트워크 지연으로 인한 것일 가능성이 있으며, 알림을 안전하게 무시할 수 있습니다.

추가 확인을 위해 마지막으로 CLI에서 `enginestatus all` 명령을 실행하고 엔진 및 규칙이 성공적으로 업데이트되고 있는지 확인할 수 있습니다. 엔진은 규칙보다 자주 업데이트되지 않습니다. 따라서 최근 5-10분 내에 마지막으로 업데이트된 규칙을 볼 수 있지만 마지막 엔진 업데이트 이후 며칠 또는 몇 주가 될 수 있습니다.

```
<#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

해결 중

네트워크 연결

실패가 계속 발생하는 경우 추가 트러블슈팅을 위해 우리가 할 수 있는 몇 가지 사항이 있습니다.

1. 빌드와 일치하는 해당 AsyncOS 버전 내에서 방화벽 인덱스를 검토하고 몇 가지 기본 네트워크 연결 테스트를 수행합니다. 다음은 성공적인 Connected 세션을 보여주는 몇 가지 텔넷 테스트입니다. 이것이 바로 저희가 찾고 있는 것입니다.
 1. [AsyncOS 16.0](#)에 사용할 수 있는 제품을 보려면 여기를 클릭하십시오.
 2. 하나 이상의 테스트가 실패할 경우 네트워크에서 이 트래픽을 아웃바운드로 허용했는지 확인하고 재시도해야 합니다.

```
<#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.
```

매니페스트 서버 사용

1. update-manifests.ironport.com은 물리적 어플라이언스에 사용되고 update-manifests.sco.cisco.com은 가상에 사용됩니다. 올바른 호스트가 사용 중인지 확인하기 위해 updateconfig 명령과 dynamichost를 실행합니다. 잘못된 경우 hostname:port를 수정한 다음 변경 사항을 커밋하고 저장하십시오.

```
<#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

단계를 거쳤지만 업데이트 실패가 계속 발생하는 경우 Cisco TAC 케이스 열기를 계속 진행해 주시면 도와드리겠습니다.

관련 정보

- [Cisco Secure Email Cloud Gateway 최종 사용자 설명서](#)
- [Cisco Secure Email Gateway 최종 사용자 설명서](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.