ESA 중앙 집중화 정책, 바이러스 및 PVO(Outbreak Quarantine)를 활성화할 수 없음

목차

소개

이 문서에서는 Enable(활성화) 버튼이 회색으로 비활성화되어 문제 해결 방법을 제공하므로 Cisco ESA(Email Security Appliance)에서 중앙 집중화 정책, 바이러스 및 신종 바이러스 격리(PVO)를 활성화할 수 없는 문제에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SMA(Security Management Appliance)에서 PVO를 활성화하는 방법.
- 관리되는 각 ESA에 PVO 서비스를 추가하는 방법
- PVO 마이그레이션을 구성하는 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SMA 버전 8.1 이상
- ESA 버전 8.0 이상

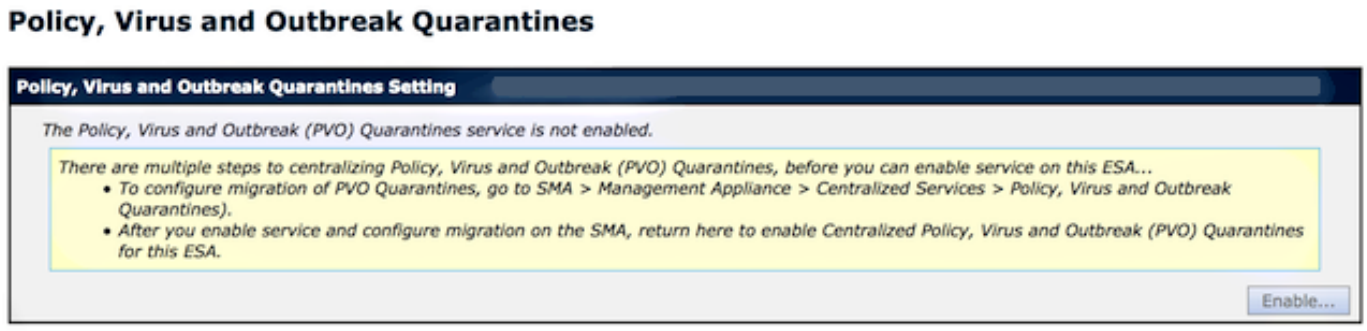
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

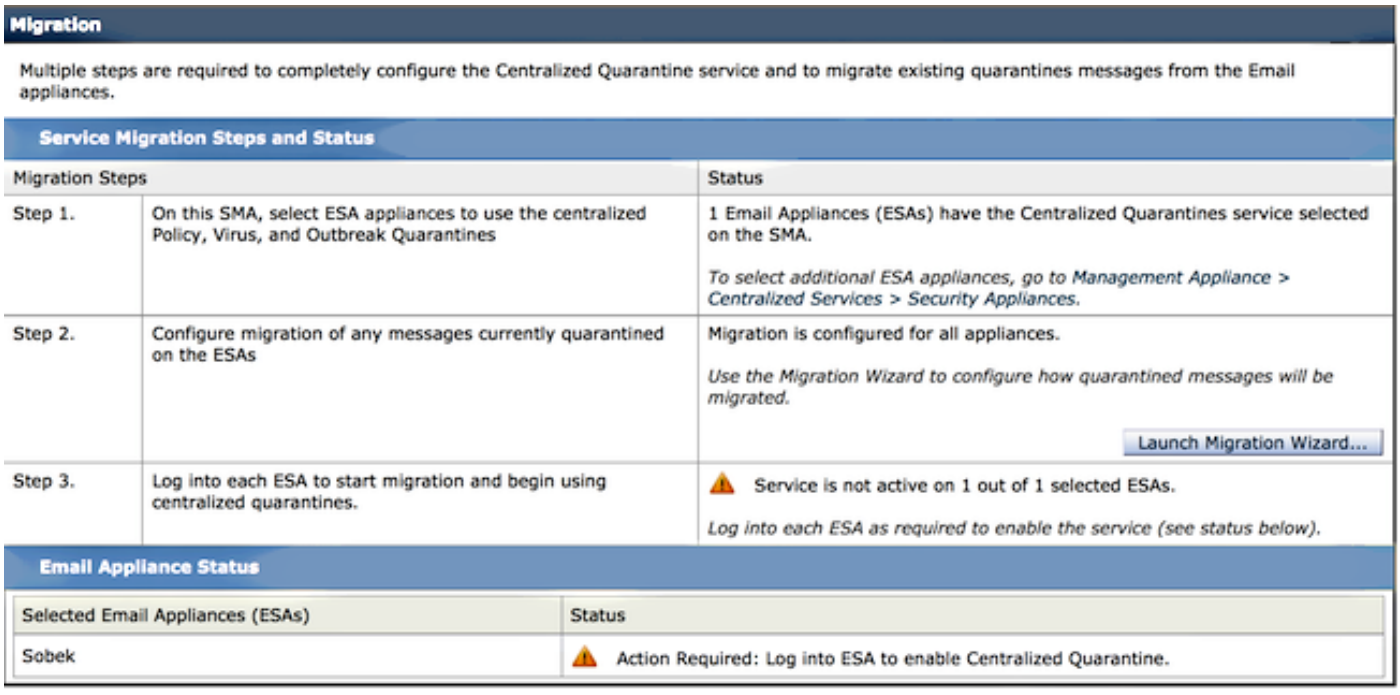
ESA에서 특정 필터, 정책 및 스캐닝 작업에서 처리하는 메시지는 추가 조치를 위해 일시적으로 격리될 수 있습니다.경우에 따라 SMA에 PVO가 올바르게 구성되고 마이그레이션 마법사가 사용되었지만 ESA에서 PVO를 활성화할 수 없는 경우가 있습니다.ESA가 포트 7025의 SMA에 연결할 수 없기 때문에 ESA에서 이 기능을 활성화하는 버튼은 일반적으로 회색으로 표시됩니다.

문제

ESA에서 Enable(활성화) 버튼이 회색으로 표시됩니다.



SMA는 서비스가 활성 상태가 아니며 필요한 조치를 보여줍니다.



솔루션

여기에 설명된 몇 가지 시나리오가 있습니다.

시나리오 1

SMA에서 어플라이언스가 온라인 상태인지 확인하기 위해 CLI에서 **status** 명령을 실행합니다 .SMA가 오프라인 상태이면 연결이 실패하여 ESA에서 PVO를 활성화할 수 없습니다.

```
sma.example.com> status

Enter "status detail" for more information.

Status as of:                  Mon Jul 21 11:57:38 2014 GMT
Up since:                      Mon Jul 21 11:07:04 2014 GMT (50m 34s)
Last counter reset:            Never
System status:                 Offline
Oldest Message:                No Messages
```

SMA가 오프라인 상태인 경우 **resume** 명령을 실행하여 다시 온라인으로 전환하여 cpq_listener를 시작합니다.

```
sma.example.com> resume

Receiving resumed for euq_listener, cpq_listener.
```

시나리오 2

SMA에서 마이그레이션 마법사를 사용한 후에는 변경 사항을 커밋하는 것이 중요합니다.변경 사항을 커밋하지 않으면 ESA의 [Enable...] 버튼이 회색으로 표시됩니다.

1. SMA 및 ESA에 로그인합니다. **운영자**(또 다른 계정 유형)나 설정을 수행할 수 있는 것이 아니라 관리자 계정 또는 ESA 측에서 [Enable..] 버튼이 회색으로 표시됩니다.

2. SMA에서 Management Appliance(**관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 Outbreak 격리)를** 선택합니다.

3. Launch **Migration Wizard(마이그레이션 마법사 실행**)를 클릭하고 마이그레이션 방법을 선택합니다.

4. 변경 사항**을 제출하고** 커밋합니다.

시나리오 3

ESA가 deliveryconfig 명령을 통해 기본 전달 인터페이스로 구성되었고 SMA에 대한 연결이 없는 경우 SMA가 다른 서브넷에 있거나 경로가 없기 때문에 기본 인터페이스에는 SMA에 대한 연결이 없는 경우 ESA에서 PVO를 활성화할 수 없습니다.

다음은 인터페이스로 구성된 기본 전달 인터페이스가 있는 ESA**입니다**.

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In
```

인터페이스 In에서 SMA 포트 7025로의 ESA 연결 테스트는 다음과 같습니다.

```
mx.example.com> telnet

Please select which interface you want to telnet from.
1. Auto
2. In (192.168.1.1/24: mx.example.com)
3. Management (10.172.12.18/24: mgmt.example.com)
[1]> 2

Enter the remote hostname or IP address.
[]> 10.172.12.17

Enter the remote port.
[25]> 7025

Trying 10.172.12.17...
telnet: connect to address 10.172.12.17: Operation timed out
telnet: Unable to connect to remote host
```

이 문제를 해결하려면 ESA에서 정확한 인터페이스를 자동으로 사용하는 **자동**으로 기본 인터페이스를 구성합니다.

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In

Choose the operation you want to perform:
- SETUP - Configure mail delivery.
[]> setup

Choose the default interface to deliver mail.
1. Auto
2. In (192.168.1.1/24: mx.example.com)
3. Management (10.172.12.18/24: mgmt.example.com)
[1]> 1
```

시나리오 4

중앙 집중식 격리에 대한 연결은 기본적으로 TLS(Transport Layer Security)로 암호화됩니다 .ESA에서 메일 로그 파일을 검토하고 SMA에서 포트 7025에 대한 DCID(Delivery Connection ID)를 검색하는 경우 다음과 같은 TLS 실패 오류가 표시될 수 있습니다.

```
Mon Apr 7 15:48:42 2014 Info: New SMTP DCID 3385734 interface 172.16.0.179
address 172.16.0.94 port 7025
Mon Apr 7 15:48:42 2014 Info: DCID 3385734 TLS failed: verify error: no certificate
from server
Mon Apr 7 15:48:42 2014 Info: DCID 3385734 TLS was required but could not be
successfully negotiated
```

ESA CLI에서 **tlsverify**를 실행하면 동일한 내용이 표시됩니다.

```
mx.example.com> tlsverify

Enter the TLS domain to verify against:
[]> the.cpq.host

Enter the destination host to connect to.  Append the port (example.com:26) if you are not
connecting on port 25:
[the.cpq.host]> 10.172.12.18:7025

Connecting to 10.172.12.18 on port 7025.
Connected to 10.172.12.18 from interface 10.172.12.17.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher ADH-CAMELLIA256-SHA.
Verifying peer certificate.
Certificate verification failed: no certificate from server.
TLS connection to 10.172.12.18 failed: verify error.
TLS was required but could not be successfully negotiated.

Failed to connect to [10.172.12.18].
TLS verification completed.
```

이를 기반으로 SMA와 협상하기 위해 사용되는 ADH-CAMELOPE256-SHA 암호화로 인해 SMA가 피어 인증서를 제공하지 못합니다.추가 조사를 통해 모든 ADH 암호가 피어 인증서를 제공하지 않는 익명 인증을 사용한다는 사실을 확인할 수 있습니다.**여기서 해결 방법은 익명 암호를 제거하는 것입니다**.이렇게 하려면 발신 암호 목록을 HIGH:MEDIUM:ALL:-aNULL:-SSLv2로 변경합니다.

```
mx.example.com> sslconfig

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> OUTBOUND

Enter the outbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]>

Enter the outbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> HIGH:MEDIUM:ALL:-aNULL:-SSLv2

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
```

```
 Outbound SMTP ciphers: HIGH:MEDIUM:ALL:-aNULL:-SSLv2

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>

mx.example.com> commit
```

팁:또한 **-SSLv2**는 안전하지 않은 암호이므로 추가합니다.

시나리오 5

PVO를 활성화할 수 없으며 이 유형의 오류 메시지가 표시됩니다.

```
Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines
configuration as host1 and host2 in Cluster have content filters / DLP actions
available at a level different from the cluster Level.
```

오류 메시지는 호스트 중 하나에 DLP 기능 키가 적용되지 않았고 DLP가 비활성화되었음을 나타낼 수 있습니다.이 솔루션은 누락된 기능 키를 추가하고 기능 키가 적용된 호스트와 동일한 DLP 설정을 적용하는 것입니다.이 기능 키 불일치는 Outbreak Filter, Sophos Antivirus 및 기타 기능 키와 동일한 영향을 미칠 수 있습니다.

시나리오 6

클러스터 컨피그레이션에서 콘텐츠, 메시지 필터, DLP 및 DMARC 설정에 대한 머신 또는 그룹 레벨 컨피그레이션이 있는 경우 PVO에 대한 활성화 버튼이 회색으로 표시됩니다.이 문제를 해결하려면 DLP 및 DMARC 설정은 물론 모든 메시지 및 콘텐츠 필터를 시스템 또는 그룹 수준에서 클러스터 레벨로 이동해야 합니다.또는 클러스터에서 시스템 레벨 컨피그레이션이 있는 시스템을 완전히 제거할 수 있습니다.클러스터 컨피그레이션을 상속하려면 CLI 명령 clusterconfig > **removemachine**을 입력한 다음 클러스터에 다시 조인합니다.

관련 정보

- SMA에서 PVO 격리에 대한 전달 문제 해결
- ESA가 클러스터링된 경우 PVO 마이그레이션 마법사의 요구 사항
- 기술 지원 및 문서 – Cisco Systems