Secure Malware Analytics(이전의 Threat Grid) Appliance를 모니터링하도록 원격 Prometheus 및 Grafana를 구성하는 방법

목차

소개

SMA(Secure Malware Analytics) Appliance에서는 어플라이언스 리소스 사용을 모니터링하는 데 SNMP 프로토콜을 제공하지 않습니다. 대신 어플라이언스에서 Prometheus를 제공합니다.

이 문서에서는 원격 Prometheus 인스턴스를 구성하고 Grafanato를 사용하여 어플라이언스에서 가져온 데이터를 시각화하는 방법을 설명합니다.

사전 요구 사항

다음 도구를 다운로드하여 로컬 컴퓨터/서버에 설치합니다.

- 프로메테우스 -https://prometheus.io/download/
- 그라파나 -https://grafana.com/oss/grafana/

요구 사항

- SMA(Secure Malware Analytics) Appliance Software 버전 2.18 이상
- Windows 컴퓨터
- 어플라이언스 관리자(Opadmin) 콘솔에 대한 관리자 액세스
- SMA(Secure Malware Analytics) 어플라이언스 Opadmin SSL 인증서(로컬 시스템에서 신뢰함)

사용되는 구성 요소

- SMA(Secure Malware Analytics) 어플라이언스
- Windows 11 Pro 컴퓨터
- 프로메테우스

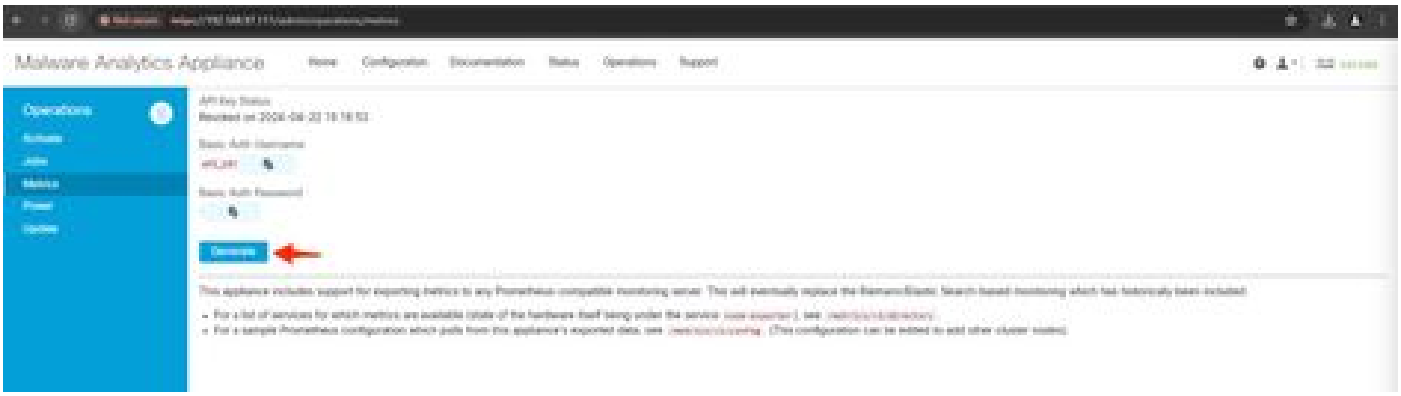
- 그라파나

구성

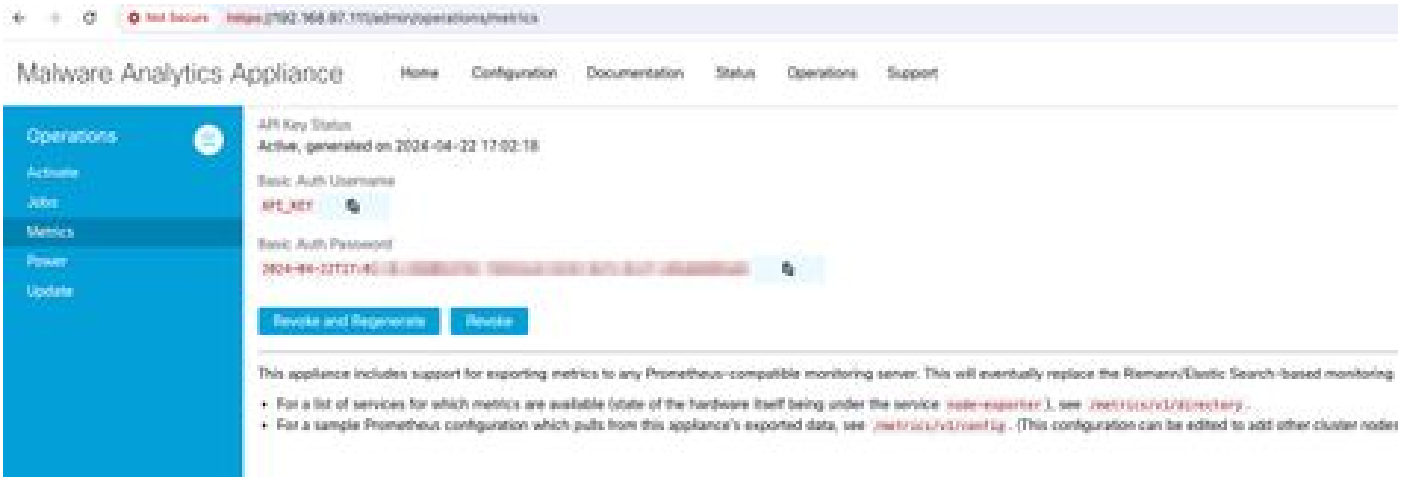
이 문서에서는 Windows 11 Pro를 Prometheus 및 Grafana를 설치한 원격 호스트로 사용했습니다. 이러한 도구는 Linux 또는 MacOS에서도 사용할 수 있습니다.

1. SMA(Secure Malware Analytics) 어플라이언스에서 API 키를 생성하여 메트릭에 액세스합니다.

SMA 어플라이언스 Opadmin에 로그인합니다. Opadmin > Operation > Metrics에서 메트릭에 대한 API 키 생성



2. 기본 인증 사용자 이름 및 비밀번호가 생성되며, 이는 Remote Prometheus 컨피그레이션에서 사용해야 합니다.



3. Prometheus 설치 및 구성

Linux 또는 MacOS를 사용 중인 경우 Prometheus 사용자 가이드에서 제공하는 지침에 따라 인스턴스를 설치합니다. 이 문서에서는 Windows 11 시스템에 Prometheus를 설치했으며, 설치 프로세스에서는 이 Youtube 비디오를 따랐습니다.

4. prometheus.ymlwith 다음 내용으로 구성 파일을 생성합니다.

```
scrape_configs:
  - job_name: metrics
```

```
    scheme: https
    file_sd_configs:
      - files:
        - 'targets.json'

    relabel_configs:
      - source_labels: [__address__]
        regex:  '[^/]+(/.*)'            # capture '/...' part
        target_label: __metrics_path__  # change metrics path
      - source_labels: [__address__]
        regex:  '([^/]+)/.*'            # capture host:port
        target_label: __address__       # change target
    basic_auth:
      username: "API_KEY"
      password: "2024-04-22T15:32:14.082689318Z xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

5. basic_auth 섹션에서 1단계에서 생성한 기본 인증 사용자 이름 및 비밀번호를 사용합니다.

6. Opadmin에 로그인한 후 UI에서 다음을 입력하여 메트릭을 가져올 수 있는 서비스의 컨피그레이션을 가져옵니다.

```
https://<opadmin IP>/metrics/v1/config
```

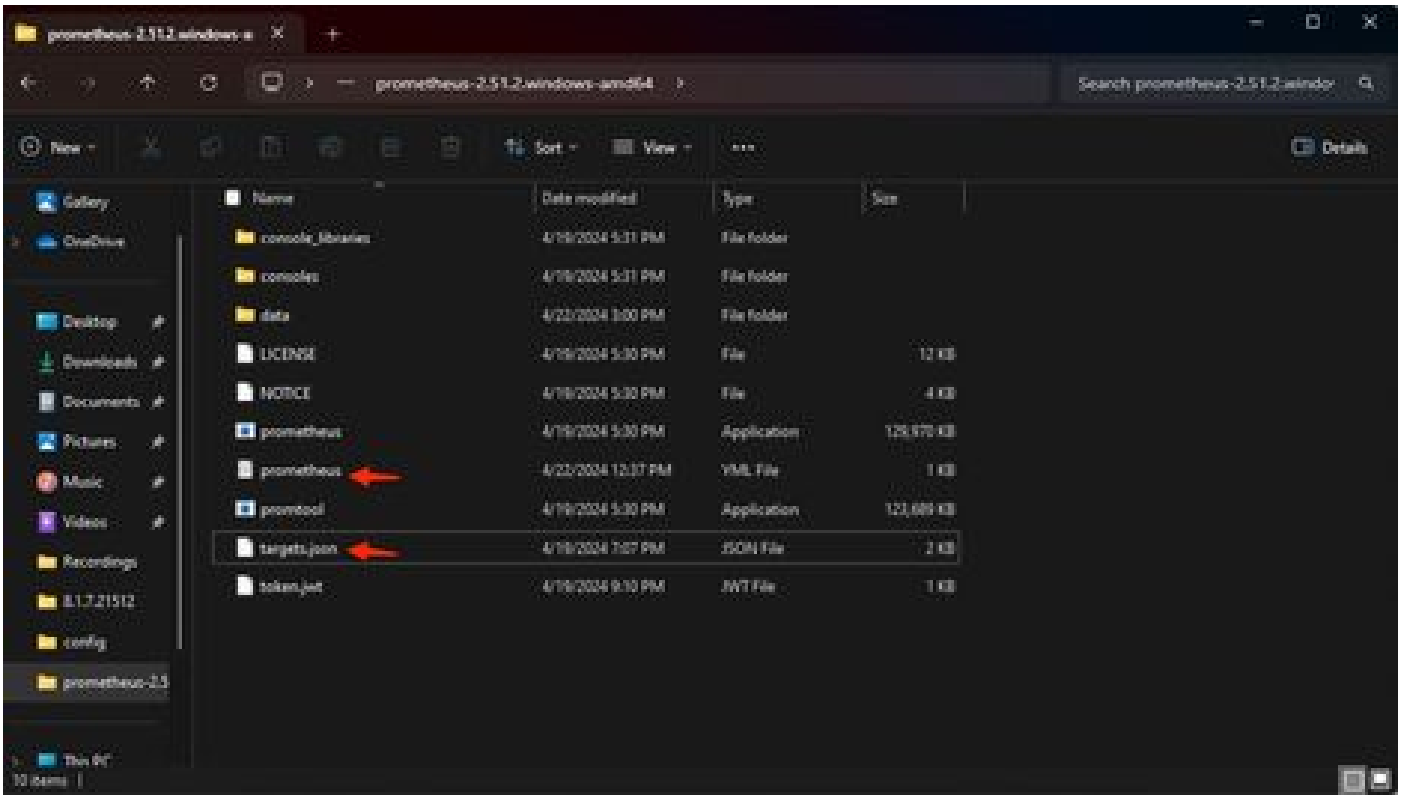
다음과 같은 기능이 제공됩니다.

```
[{"labels":{"service":"classifier"},"targets":["192.168.97.111:443/metrics/v1/service/classifier"]},{"l
```

여기서 192.168.97.111은 내 SMA 어플라이언스의 관리자 IP입니다.

7. targets.json이라는 이름의 파일을 만들고 위의 내용을 해당 파일에 복사합니다.

8. prometheus.yml 및 targets.json을 Prometheus 디렉토리에 복사합니다(설치 가이드 참조). Windows의 경우 C:\ 드라이브에 폴더를 생성하고 Prometheus 설치 파일을 압축을 풀었습니다. 그런 다음 prometheus.yml과 targets.json을 같은 폴더에 복사했습니다.



9. 프로메테우스 시작

프로메테우스를 시작하세요 Windows의 경우 명령줄에서 prometheus.exe를 실행합니다.

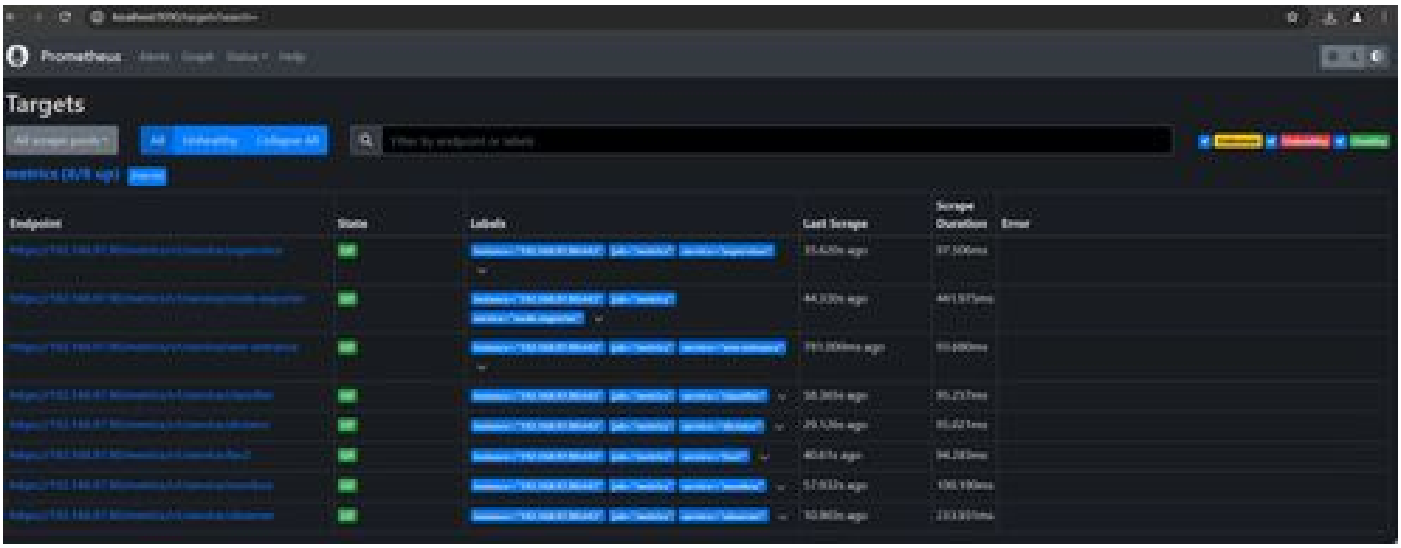
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

그러면 Prometeus가 시작되고 SMA 어플라이언스에서 메트릭을 가져오기 시작합니다. 참고: 명령줄을 닫지 마십시오. 그러면 Prometheus가 종료됩니다.

10. 로컬 Prometheus 인스턴스가 SMA 어플라이언스 로드 Prometheus UI에서 메트릭을 가져올 수 있는지 확인하려면 - `http://localhost:9090/`

11. 상태 **>** 대상으로 이동합니다. http://localhost:9090/targets?search=

몇 분 내에 모든 대상과 상태 UP를 볼 수 있습니다.



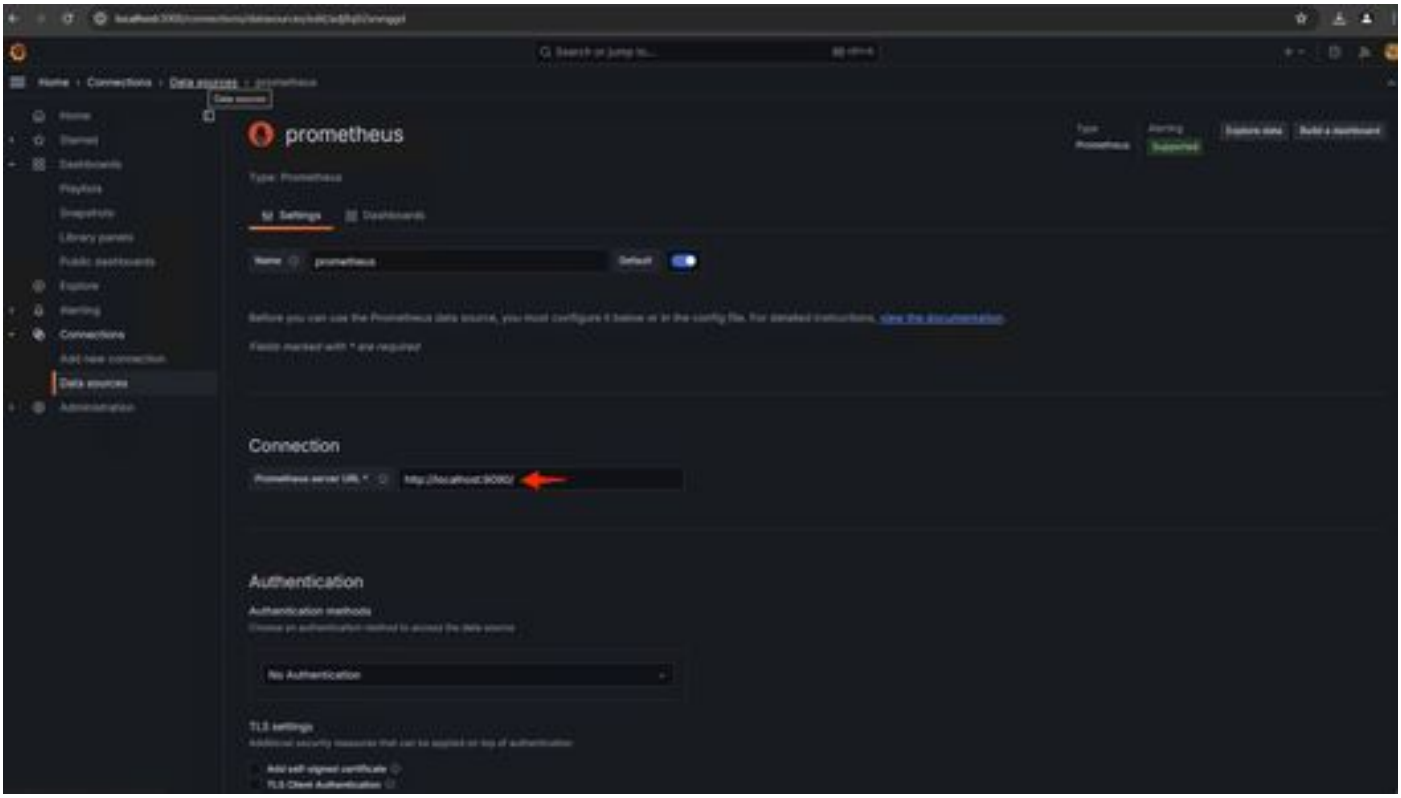
12. Grafana 설치 및 구성

Grafana Labs에서 Grafana 실행 파일을 다운로드합니다. Granafa를 설치하고 설치 프로그램에서 제공하는 지침을 따릅니다.

13. 브라우저에서 Grafana 액세스 UI를 설치한 후 -http://localhost:3000/

홈 > 연결 > 데이터 소스로 이동 - `http://localhost:3000/connections/datasources`

새 데이터 소스 추가를 선택하고 목록에서 프로메테우스를 선택합니다. Prometheus Server URL로 `http://localhost:9090/`를 입력합니다
.



해당 페이지의 하단에서 저장 및 테스트를 선택합니다. 테스트가 성공하면 대시보드를 생성할 수 있습니다.

14. Grafana 대시보드 생성

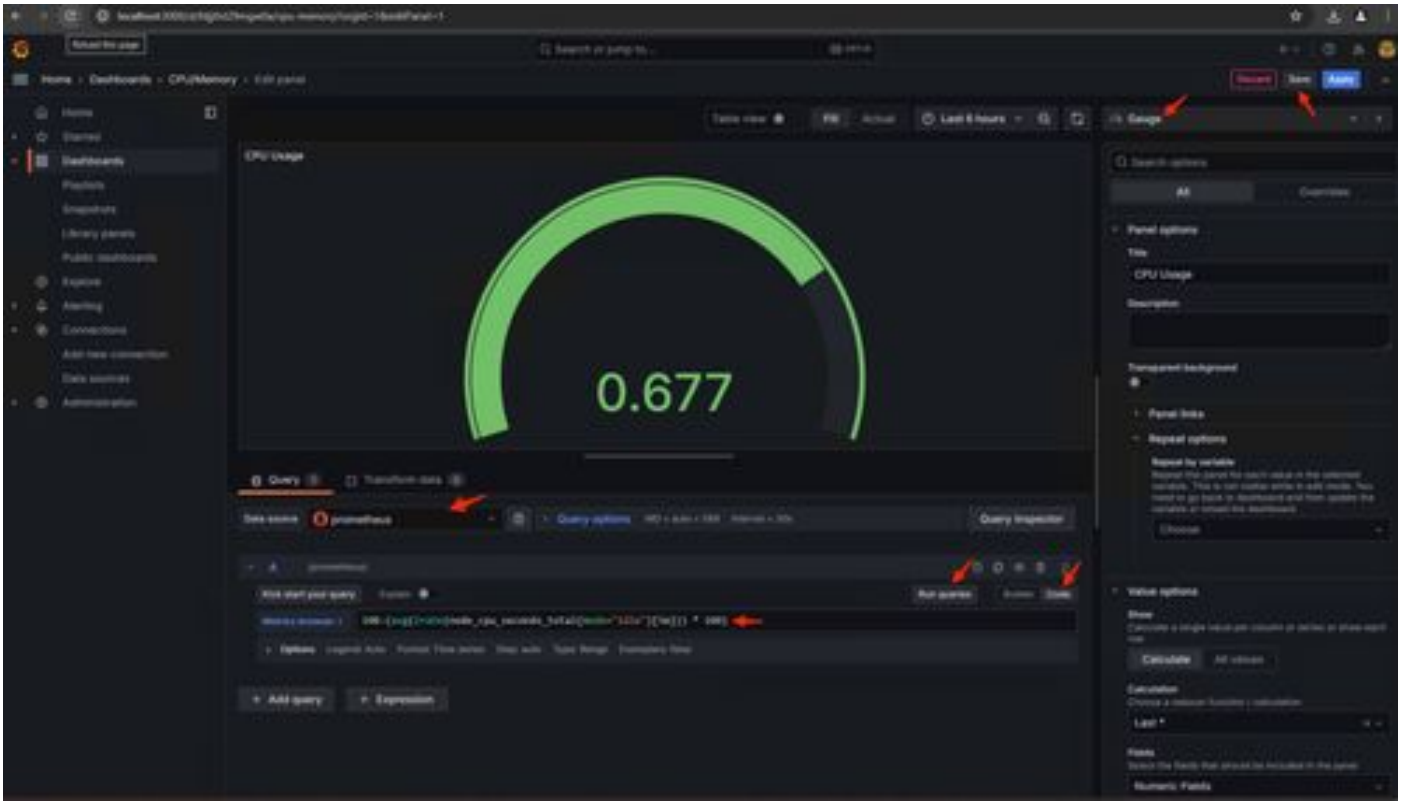
Grafana UI의 `Dashboards`로 이동하여 Create Dashboard >`Add visualization`을 선택합니다. 프로메테우스 데이터 소스를 선택합니다.

쿼리 작성기 selectCodeinput에서 시각화 유형(게이지를 선택한 경우)을 선택합니다.

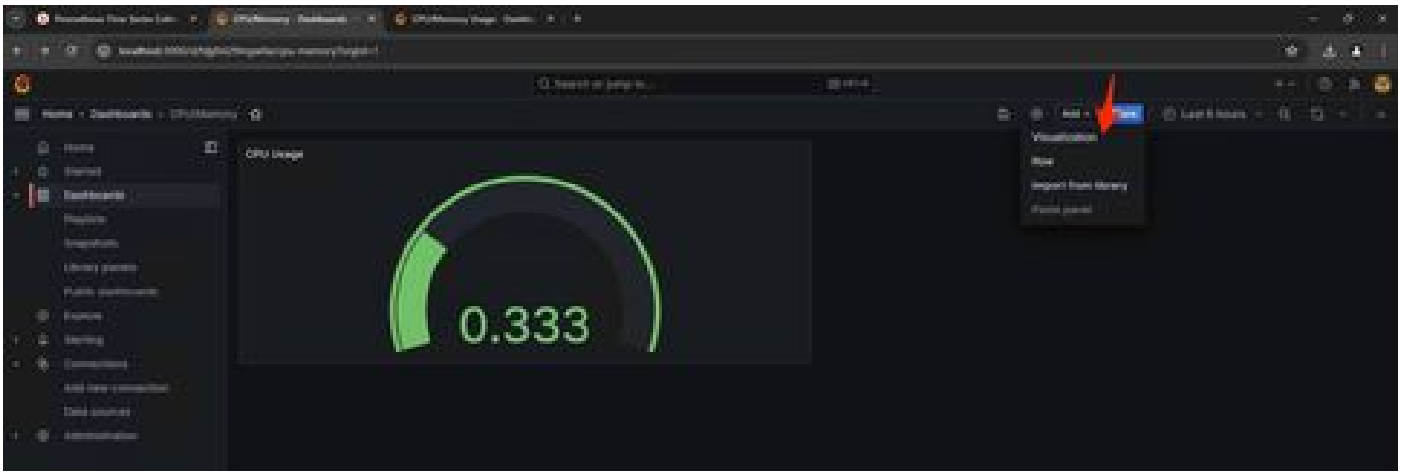
CPU 사용률에 **대한** 다음 **쿼리를 입력합니다**.

```
100-(avg(irate(node_cpu_seconds_total{mode="idle"}[5m])) * 100)
```

15. Run Queries(쿼리 실행)를 클릭하면 다음과 같은 CPU 사용량이 시각화됩니다.

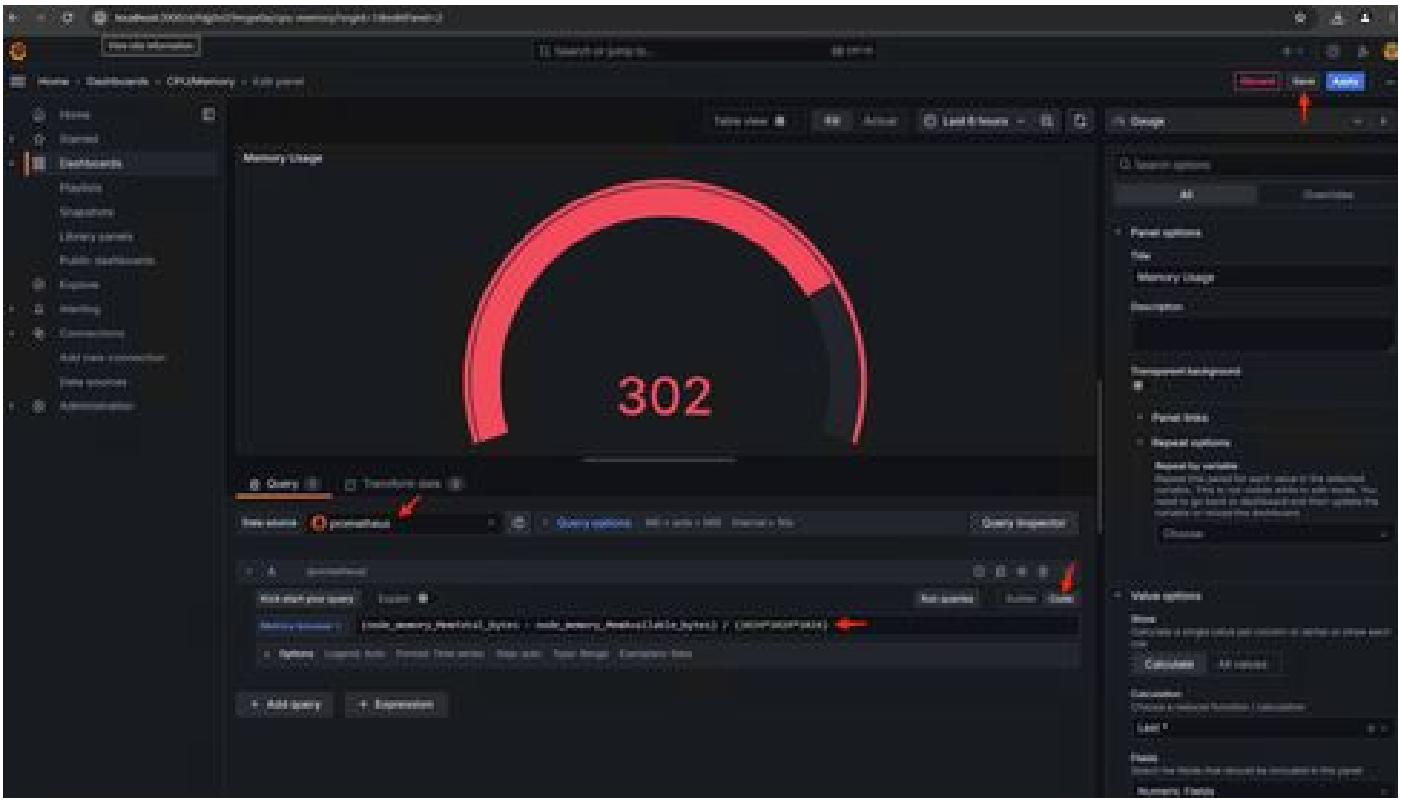


16. 패널을 저장하고 대시보드 이름을 지정한 다음 저장합니다. 메모리 사용에 대한 다른 시각화 추가 -



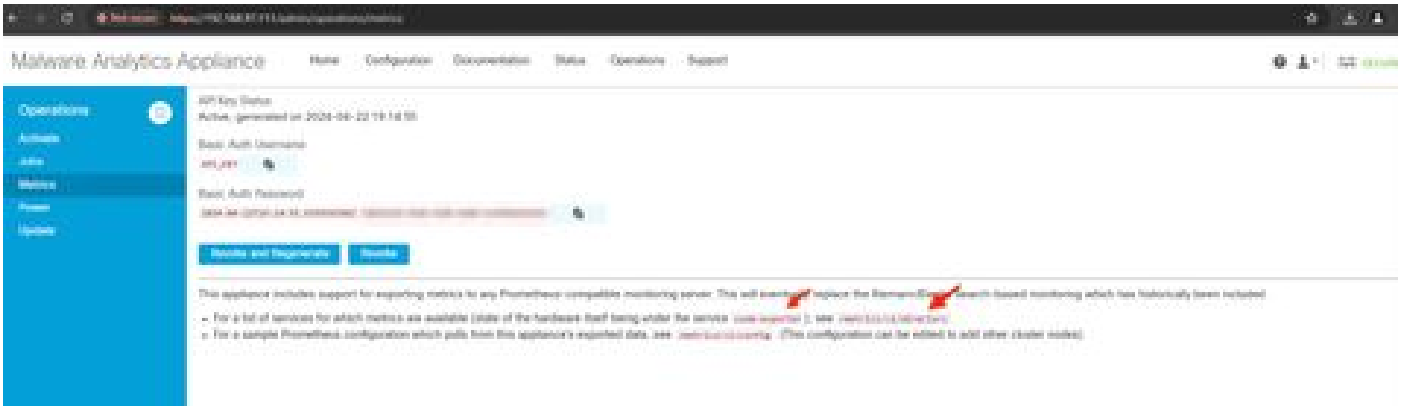
17. 메모리 사용률의 경우 다음 쿼리를 사용합니다

```
(node_memory_MemTotal_bytes - node_memory_MemAvailable_bytes) / (1024*1024*1024)
```



18. 변경사항을 저장하면 다음과 같은 대시보드가 있어야 합니다.

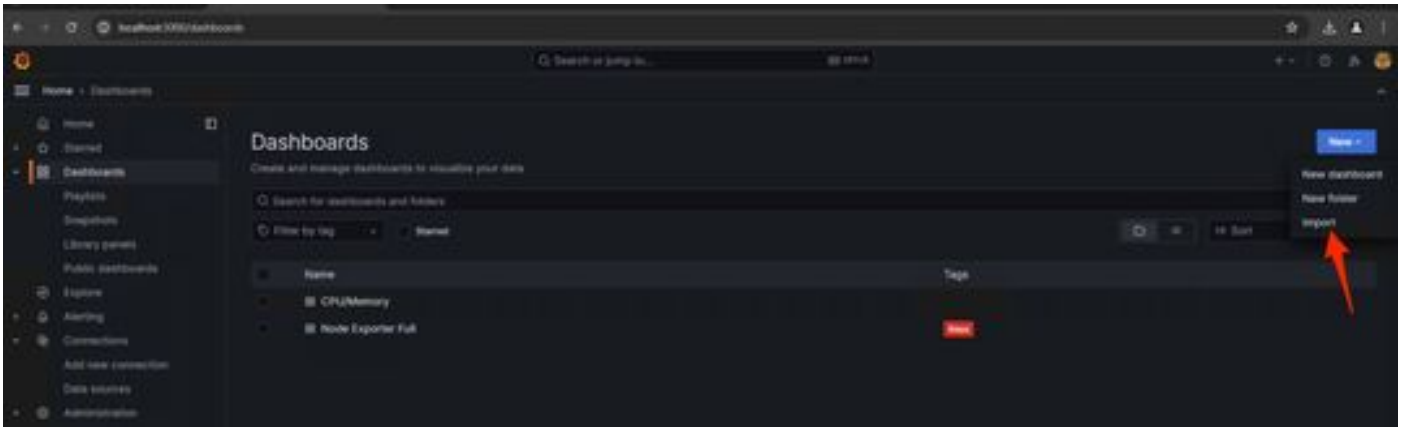
19. 기타 하드웨어 및 소프트웨어 측정 단위를 사용할 수 있습니다. 자세한 내용을 보려면 Opadmin> `Metrics`(측정 단위) 페이지에서 제공된 링크를 클릭하십시오.



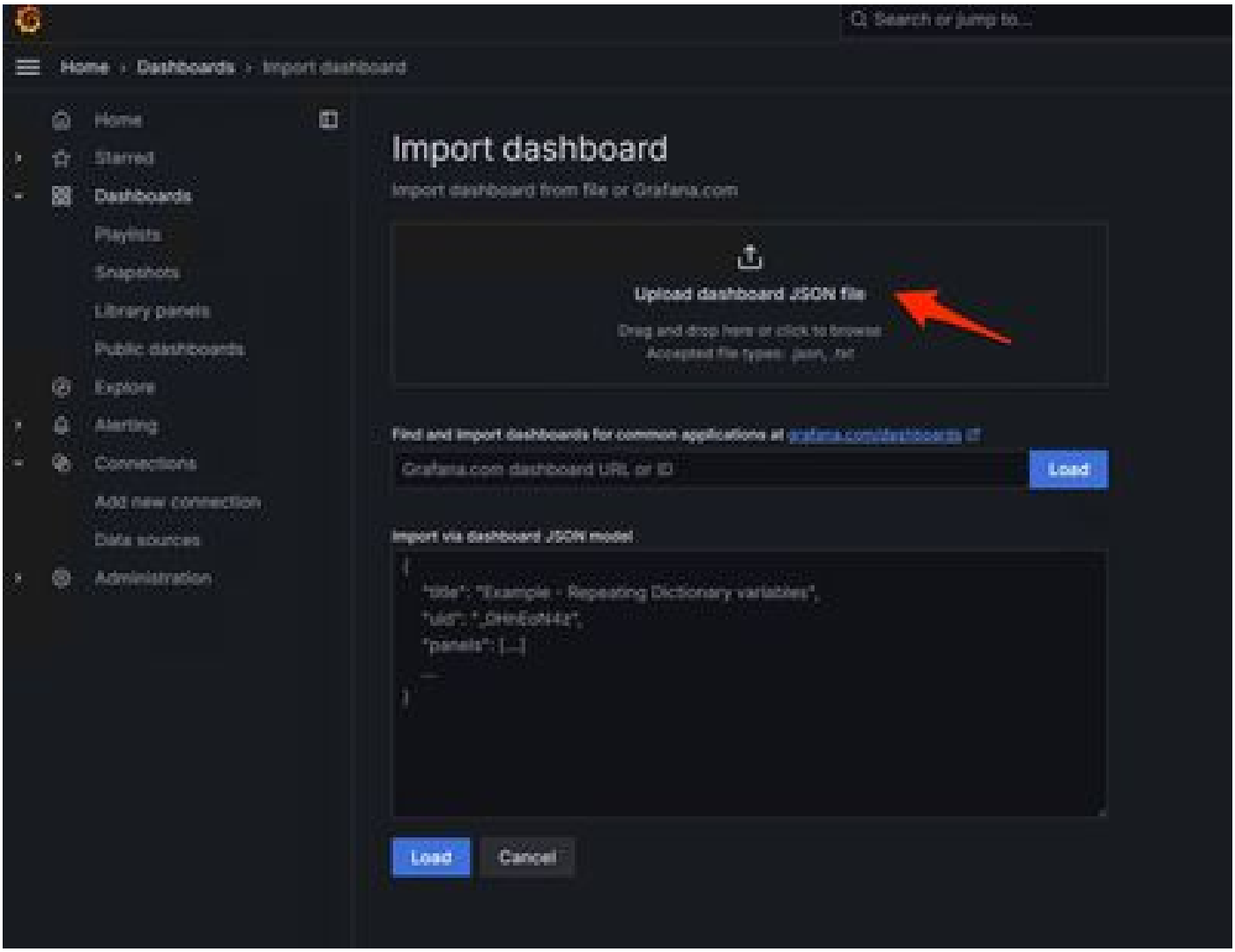
Grafana 대시보드 템플릿

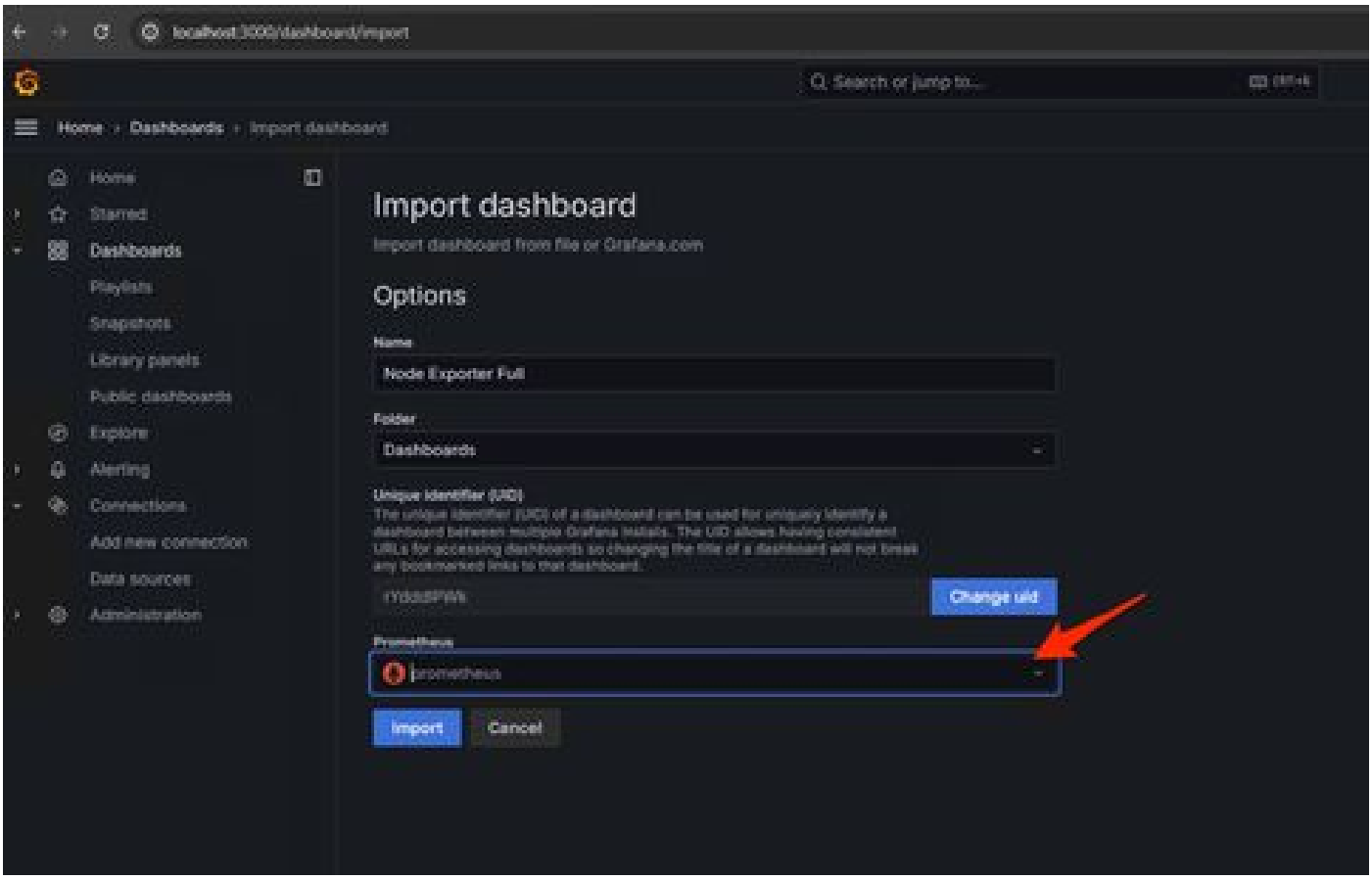
Grafana 웹 사이트에는 Node Exporter에 사용할 수 있는 Grafana Dashboard 템플릿이 많이 있습니다. 그 중 하나는 - 노드 내보내기 가득 참

1. 이 대시보드를 Grafana 인스턴스로 가져오려면 JSON을 다운로드하고 Grafana에서 JSON 파일을 가져옵니다.

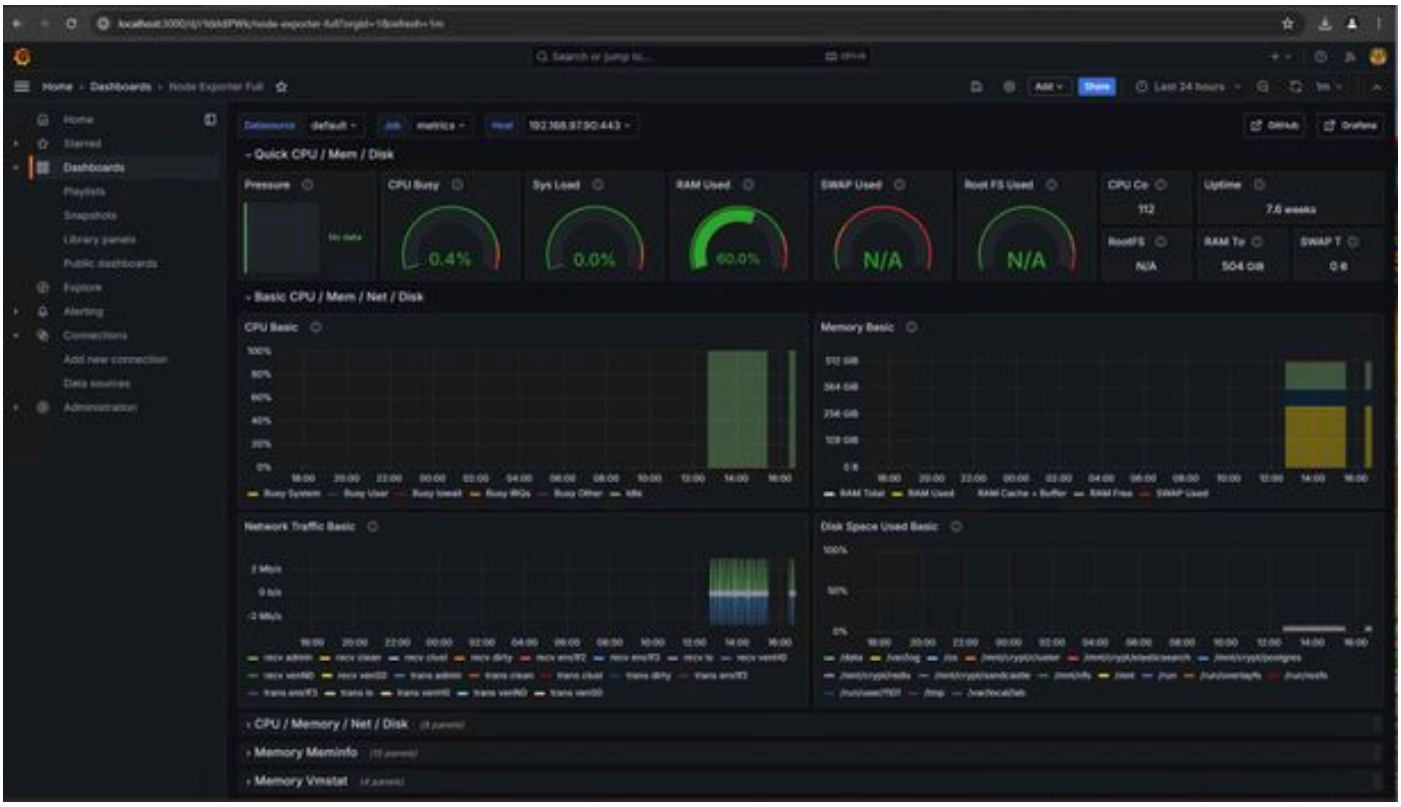


2. JSON 파일을 업로드하고 Prometheusdata 소스를 선택합니다


Search or jump to...
Home › Dashboards › Import dashboard
Home
Starred
Dashboards
Playlists
Snapshots
Library panels
Public dashboards
Explore
Alerting
Connections
Add new connection
Data sources
Administration
Import dashboard
Import dashboard from file or Grafana.com
Upload dashboard JSON file
Drag and drop here or click to browse
Accepted file types: .json, .txt
Find and import dashboards for common applications at grafana.com/dashboards
Grafana.com dashboard URL or ID
Load
Import via dashboard JSON model
{
"title": "Example - Repeating Dictionary variables",
"uid": "_DHnEoH4z",
"panels": [...]
}
Load
Cancel



3. 이렇게 하면 많은 하드웨어 정보가 포함된 대시보드가 생성됩니다(일부 패널 메트릭을 사용할 수 있는 것은 아님)-



문제 해결

Prometeus가 SMA 어플라이언스에서 메트릭을 연결 및 폴링하지 못한 경우 `Status` > Targets(상태 > 대상)에서 오류가 표시됩니다.

http://localhost:9090/targets?search=

Error가 있는 경우, 데이터를 가져오려면 먼저 오류를 수정해야 합니다. 일반적인 문제는 SMA 어플라이언스 Opadmin의 SSL 인증서가 로컬 시스템에서 신뢰되지 않는다는 것입니다. IP 및 DNS SAN을 사용하여 SMA 관리자 인증서를 만들고 서명 루트 CA를 로컬 컴퓨터의 트러스트 저장소에 추가해야 합니다.

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.