كيفية تكوين Prometheus و Grafana عن بعد لمراقبة جهاز تحليلات البرامج الضارة الآمنة (المعروفة سابقا باسم Threat Grid)

المحتويات

المقدمة

في جهاز تحليلات البرامج الضارة الآمنة (SMA)، النقد بروتوكول SNMP لمراقبة إستخدام موارد الجهاز، بل يقدم الجهاز خدمة Prometheus.

سيوضح هذا المستند كيفية تكوين مثيل Prometheus عن بعد وسيعرض UseGrafanato البيانات التي تم سحبها من الجهاز.

المتطلبات الأساسية

قم بتنزيل الأدوات التالية وتثبيتها على الجهاز/الخادم المحلي:

- برومیثیوس -https://prometheus.io/download/
- غرافانا -https://grafana.com/oss/grafana/

المتطلبات

- برنامج Secure Ware Analytics (SMA) الإصدار 2.18 والإصدارات الأحدث
- جهاز Windows
- وصول المسؤول إلى وحدة تحكم Appliance Admin(Opadmin)
- شهادة SSL الخاصة بجهاز Opadmin لتحليل البرامج الضارة الآمن (SMA) الموثوق بها بواسطة الجهاز المحلي

المكونات المستخدمة

- جهاز Secure Ware Analytics (SMA)
- جهاز Windows 11 Pro
- برومیثیوس

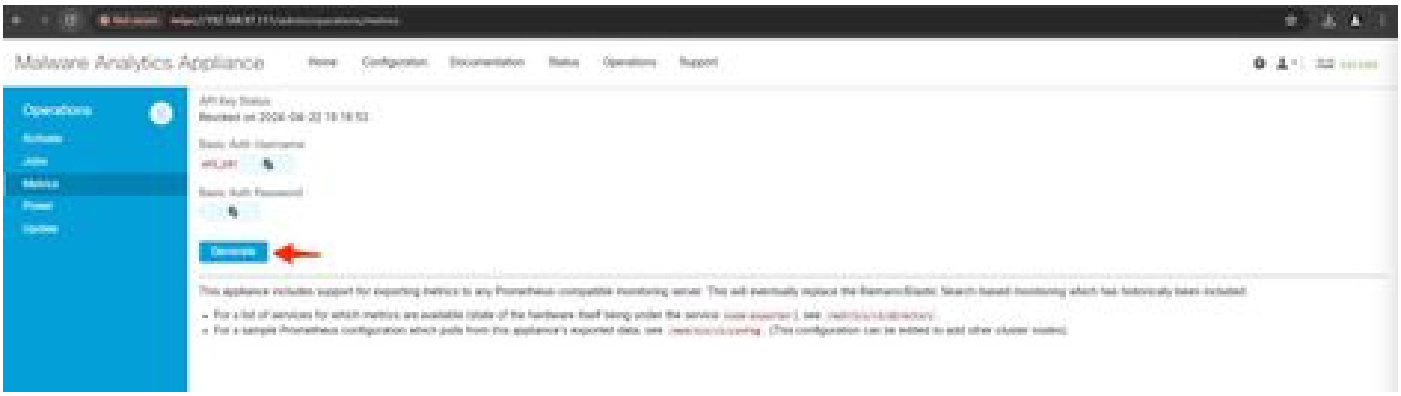
- غرافانا

التكوين

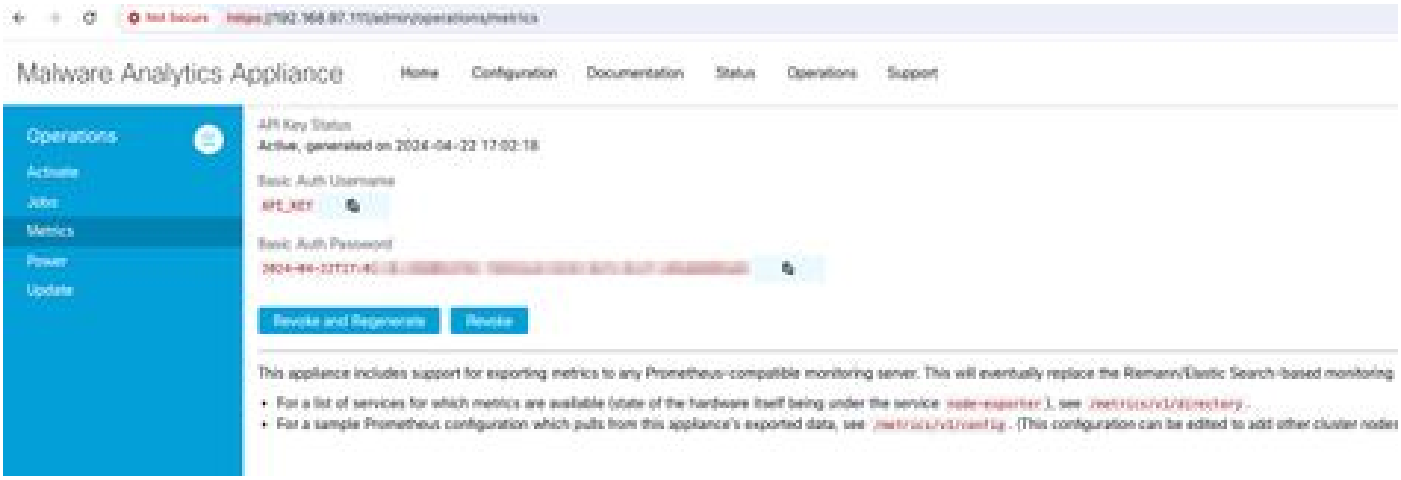
بالنسبة لهذا المستند، إستخدمنا Windows 11 Pro كمضيف بعيد حيث قمنا بتثبيت Prometheus و Grafana. هذه الأدوات متاحة أيضا ل Linux أو MacOS.

1. إنشاء مفتاح واجهة برمجة التطبيقات (API) في جهاز تحليلات البرامج الضارة الآمنة (SMA) للوصول إلى المقاييس

تسجيل الدخول إلى SMA Appliance Opadmin. توليد مفتاح API للمقاييس من OpenAdmin > العملية > المقاييس



2. سيتم إنشاء اسم مستخدم وكلمة مرور مصادقة أساسيين سيتعين علينا إستخدامهما في تكوين البرنامج البعيد.



3. تركيب وتكوين برومیثیوس

اتبع التعليمات التي تقدمها أدلة المستخدم الخاصة ببرنامج Prometheus لتثبيت التطبيق الخاص بك إذا كنت تستخدم نظام التشغيل Linux أو MacOS. لهذه الوثيقة، قمنا بتثبيت Prometheus على جهاز Windows 11، ولعملية التثبيت، اتبعنا فيديو YouTube هذا.

4. قم بإنشاء ملف تكوين باسم `prometheus.yml` يتضمن المحتوى التالي -

```
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. في قسم basic_auth، أستخدم اسم مستخدم وكلمة مرور المصادقة الأساسية التي تم إنشاؤها في الخطوة 1.

6. اسحب تكوين الخدمات التي ستتمكن من الحصول على مقاييس منها من خلال إدخال ما يلي في واجهة المستخدم بعد تسجيل الدخول إلى Opadmin -

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

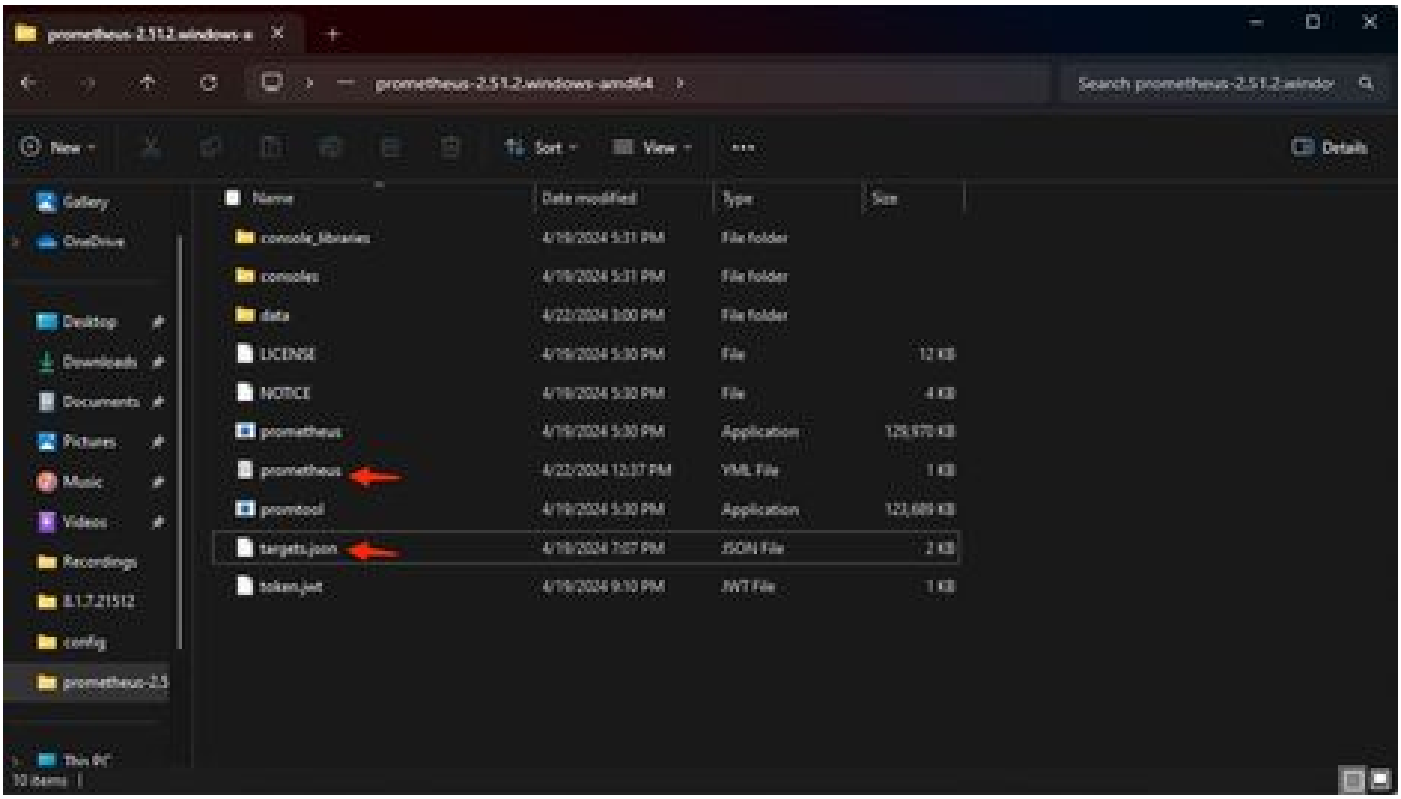
سوف تحصل على شيء مثل -

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

هنا 192.168.97.111 هو عنوان IP للمسؤول لجهاز SMA الخاص بي.

7. قم بإنشاء ملف باسم target.json وانسخ المحتوى أعلاه في هذا الملف.

8. انسخ prometheus.yml وtarget.json إلى دليل Prometheus (اتبع إرشادات التثبيت)، لـ Windows، لقد قمت بإنشاء مجلد في محرك الأقراص C:\ واستخرجت ملفات تثبيت Prometheus هناك. ثم نسخت prometheus.yml وtarget.json إلى نفس المجلد.



9. ابدأ برومیثیوس.

ابدأ برومیثیوس. بالنسبة إلى Windows، قم بتنفيذ ملف exe. من سطر الأوامر.

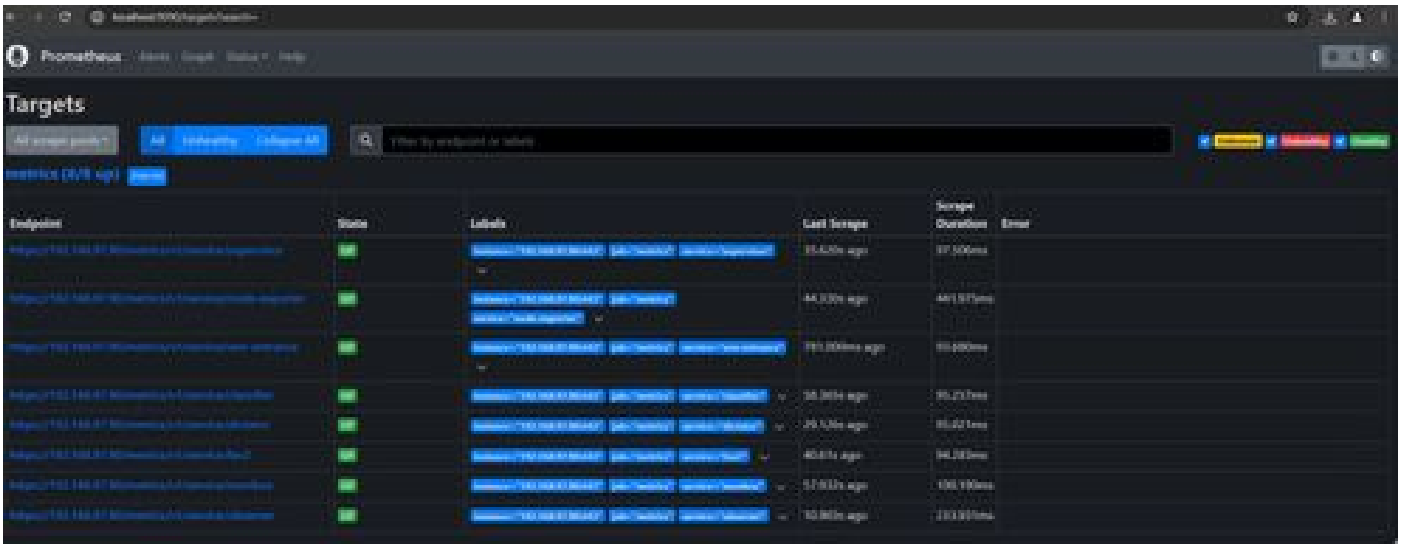
```
C:\Prometheus\prometheus-2.51.2.windows-amd64\prometheus-2.51.2.windows-amd64>prometheus.exe
```

هذا سوف يبدأ برومیثیوس ويبدأ في سحب القياسات من جهاز SMA. ملاحظة لا تغلق سطر الأوامر وإلا سيغلق برومیثیوس.

10. للتحقق مما إذا كان مثيل برومیثیوس المحلي لديك قادرا على سحب القياسات من واجهة مستخدم تحميل جهاز SMA - 'http://localhost:9090/'

11. انتقل إلى الحالة > الأهداف - http://localhost:9090/targets?search=

خالل بضع دقائق يجب أن ترى جميع الأهداف والحالة قيد التشغيل.



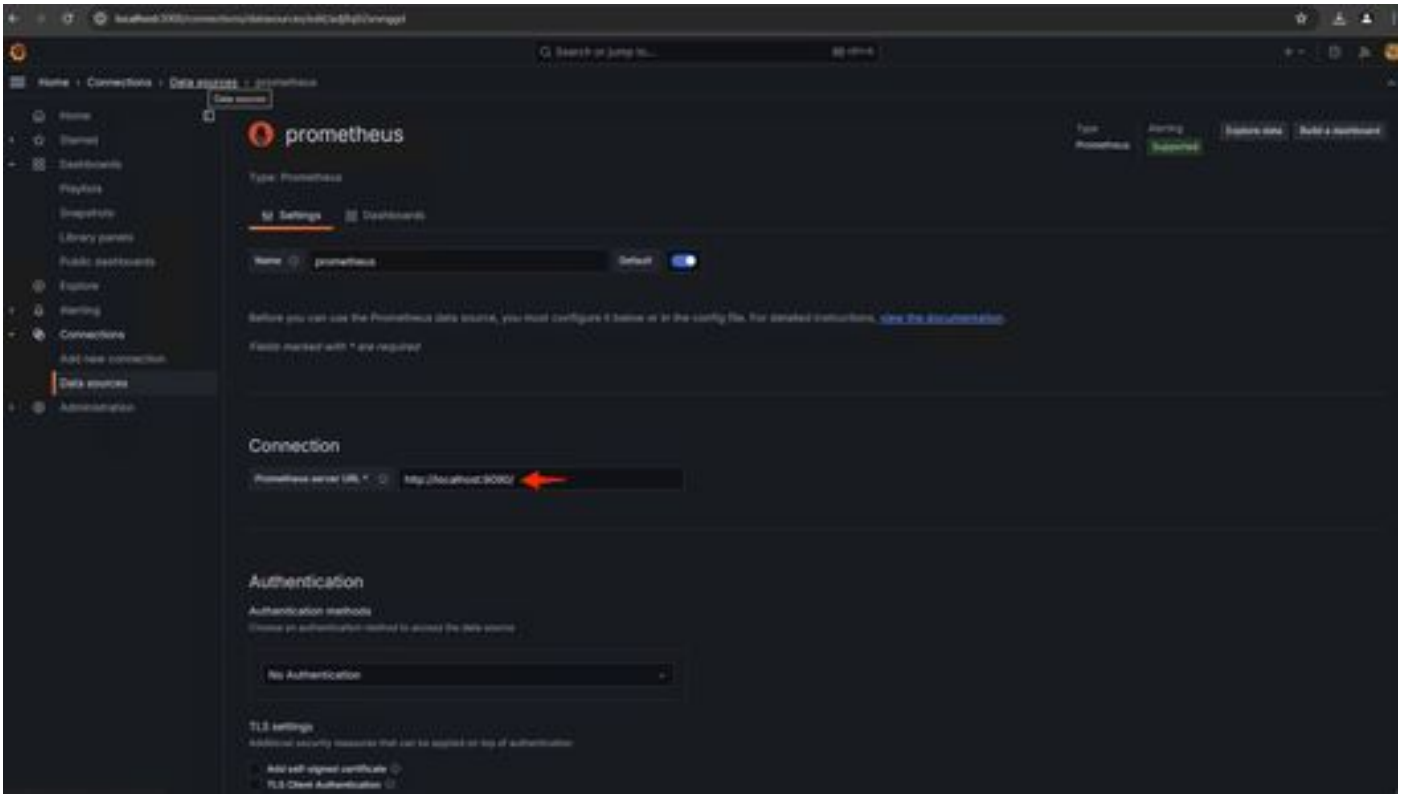
12. قم بتركيب Grafana وتكوينها

قم بتنزيل الملف التنفيذي من مختبرات Grafana. قم بتثبيت Granafa، واتبع التعليمات المقدمة من المثبت.

13. بعد تثبيت واجهة مستخدم Grafana للوصول في المستعرض - http://localhost:3000/

انتقل إلى الصفحة الرئيسية > الاتصالات > مصادر البيانات - http://localhost:3000/connections/datasources'

حدد إضافة مصدر بيانات جديد وSelectPrometheus من القائمة. أدخل 'http://localhost:9090/' كعنوان URL لخادم Prometheus



في أسفل تلك الصفحة حدد حفظ واختبار. بعد نجاح الاختبار، يمكننا إنشاء لوحة معلومات.

14. إنشاء لوحة معلومات Grafana

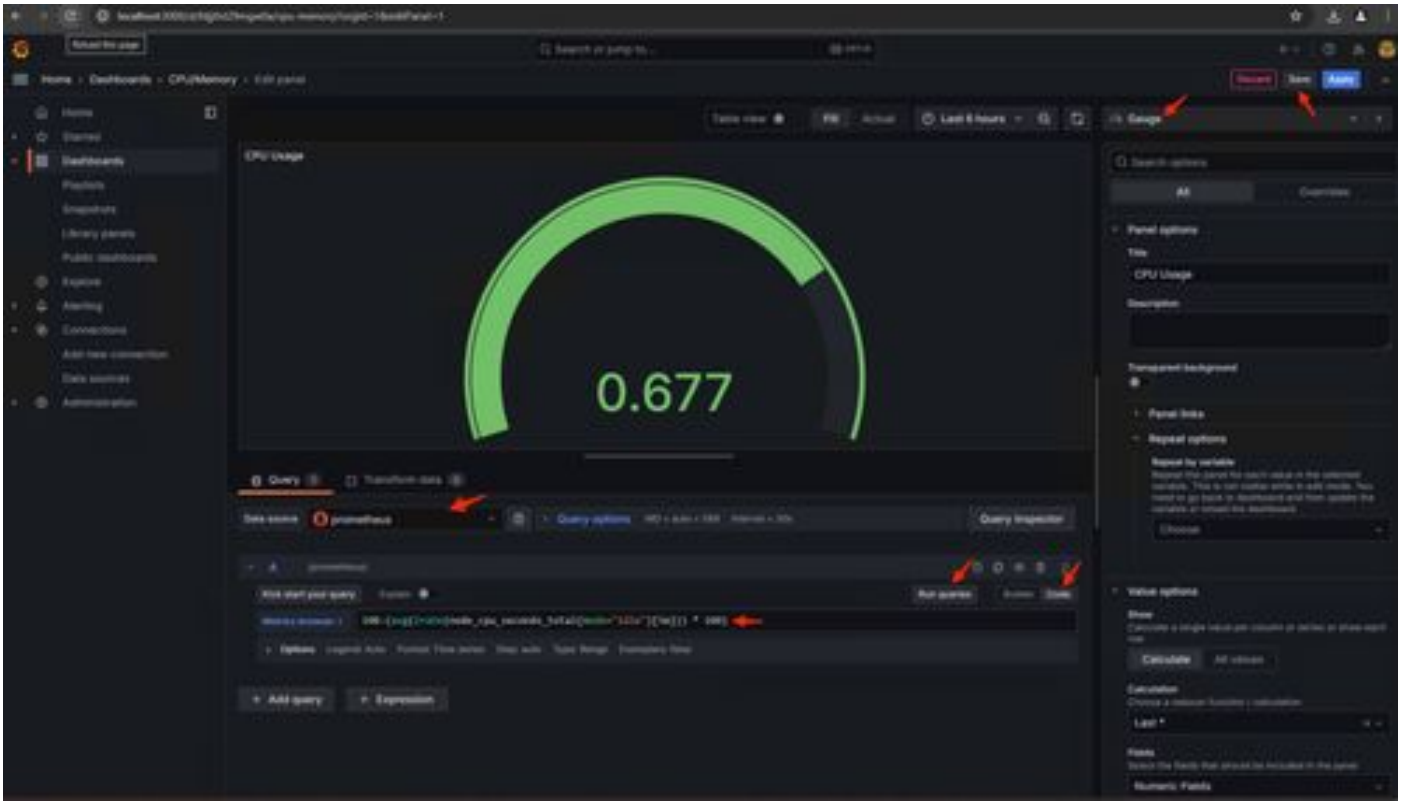
انتقل إلى لوحات المعلومات في واجهة مستخدم Grafana، حدد إنشاء لوحة المعلومات إضافة المحاكاة الافتراضية.
مصدر بيانات SelectPrometheus.

في Query Builder SelectCodeinput، حدد نوع التمثيل المرئي (أنا جاز القياس المحدد)

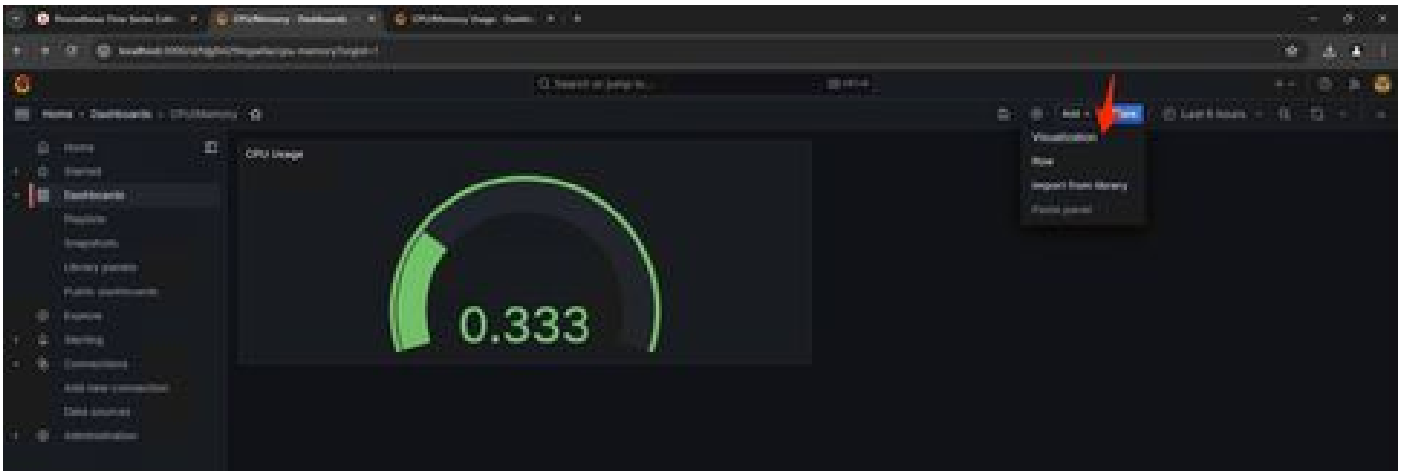
أدخل الاستعلام التالي لاستخدام وحدة المعالجة المركزية-

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

15. انقر فوق تشغيل الأسئلة ويجب أن ترى تصورا لاستخدام وحدة المعالجة المركزية مثل هذه -

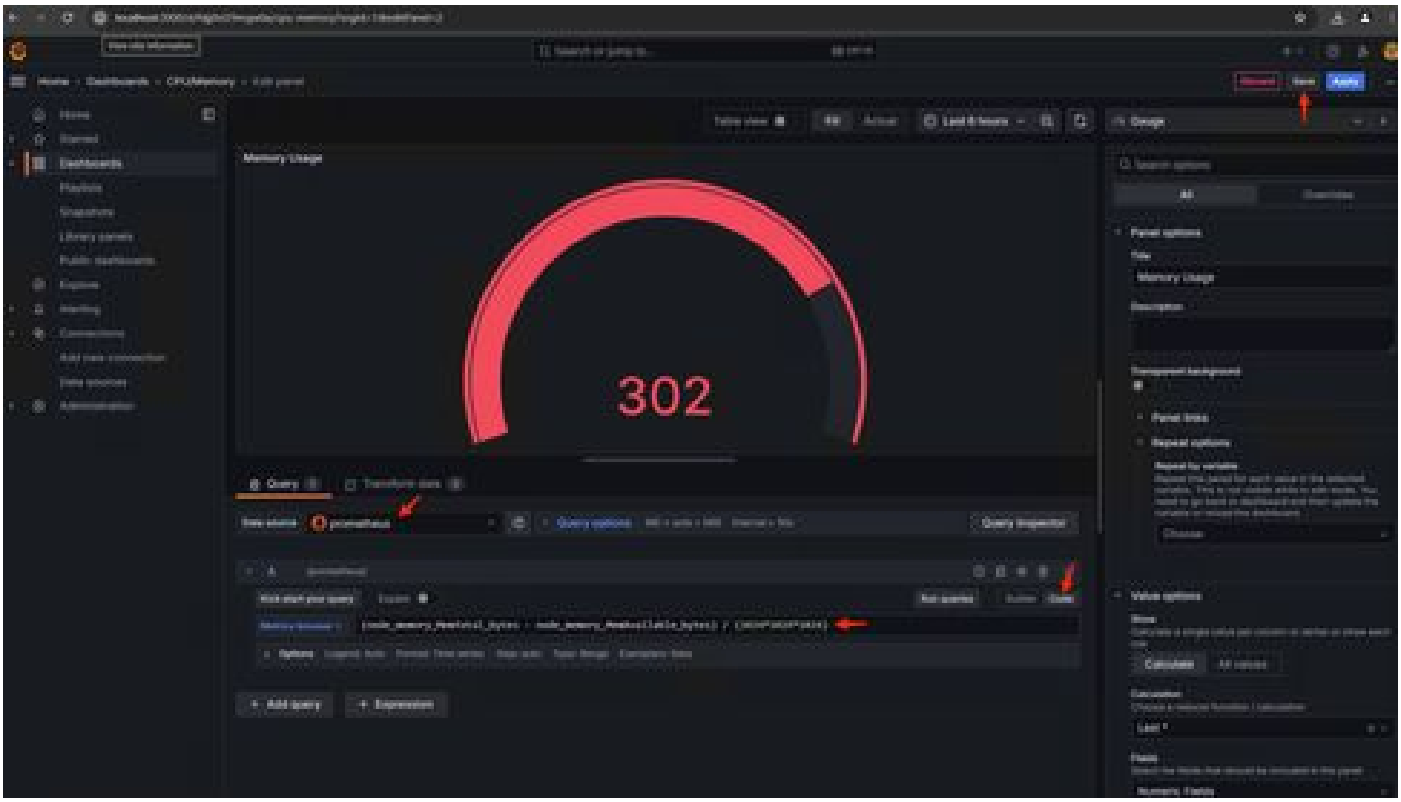


16. قم بحفظ اللوحة، وتسمية لوحة المعلومات، والحفظ. إضافة مرئيات أخرى لاستخدام الذاكرة -



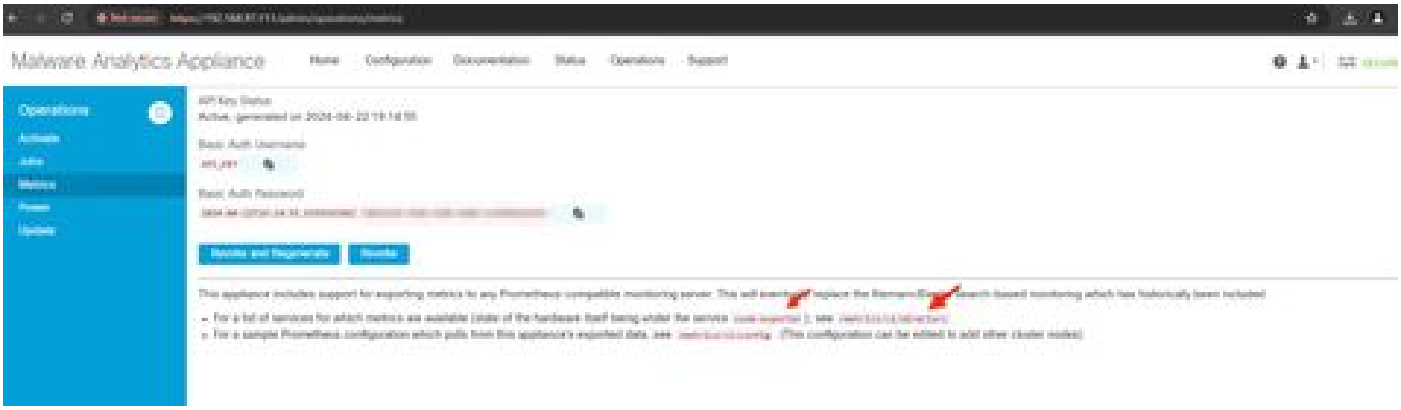
17. لاستخدام الذاكرة أستخدم الاستعلام التالي

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



18. احفظ التغييرات، ويجب أن يكون لديك لوحة معلومات كهذه -

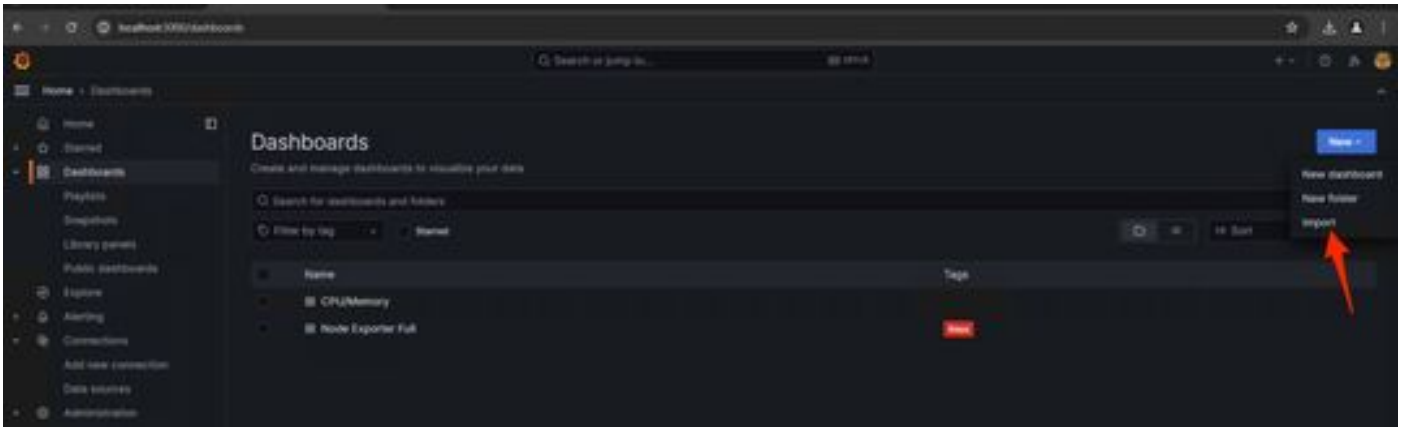
19. تتوفر مقاييس أخرى للأجهزة والبرامج، للحصول على التفاصيل انقر فوق الارتباطات المتوفرة في صفحة Opadmin>Metrics



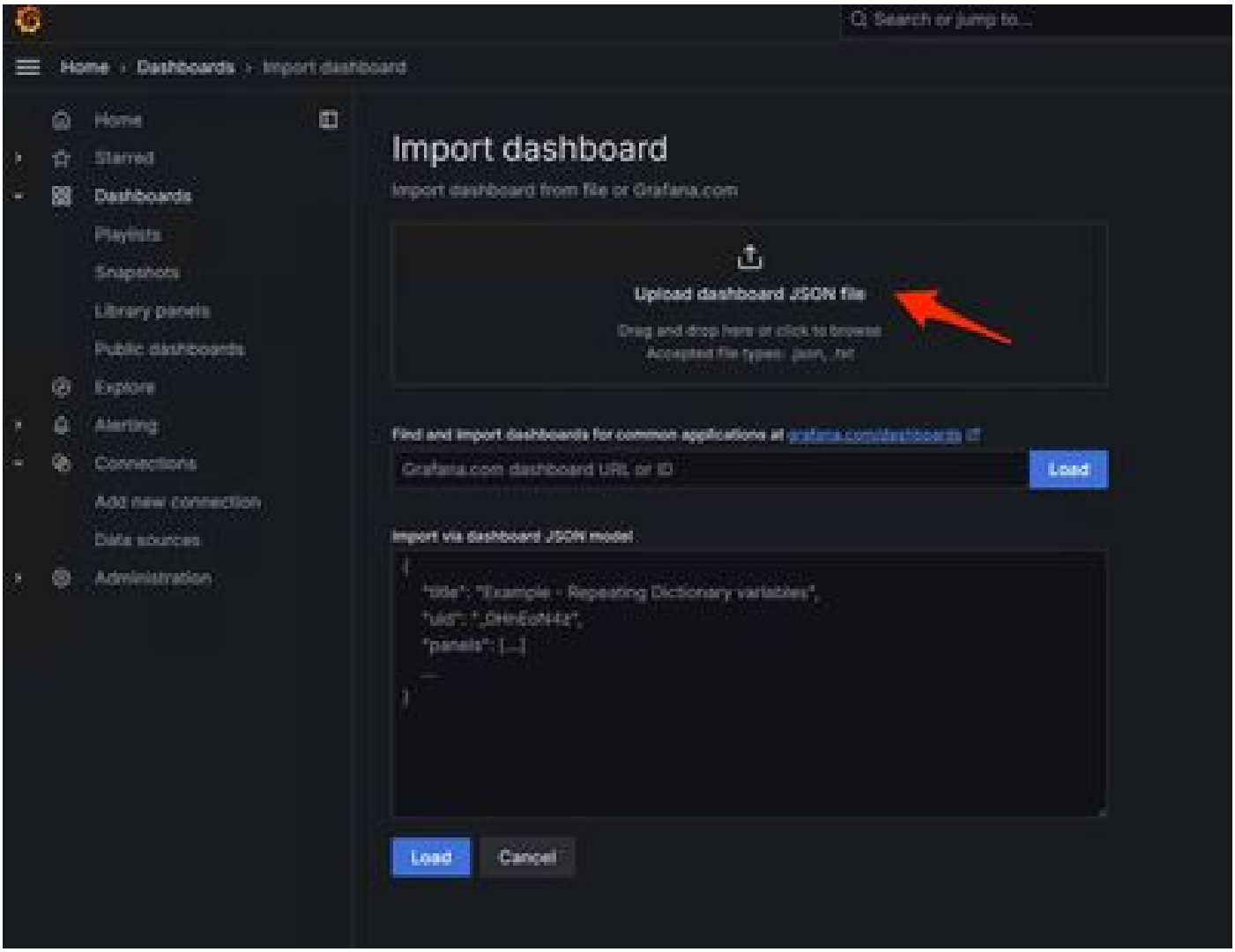
قالب لوحة معلومات Grafana

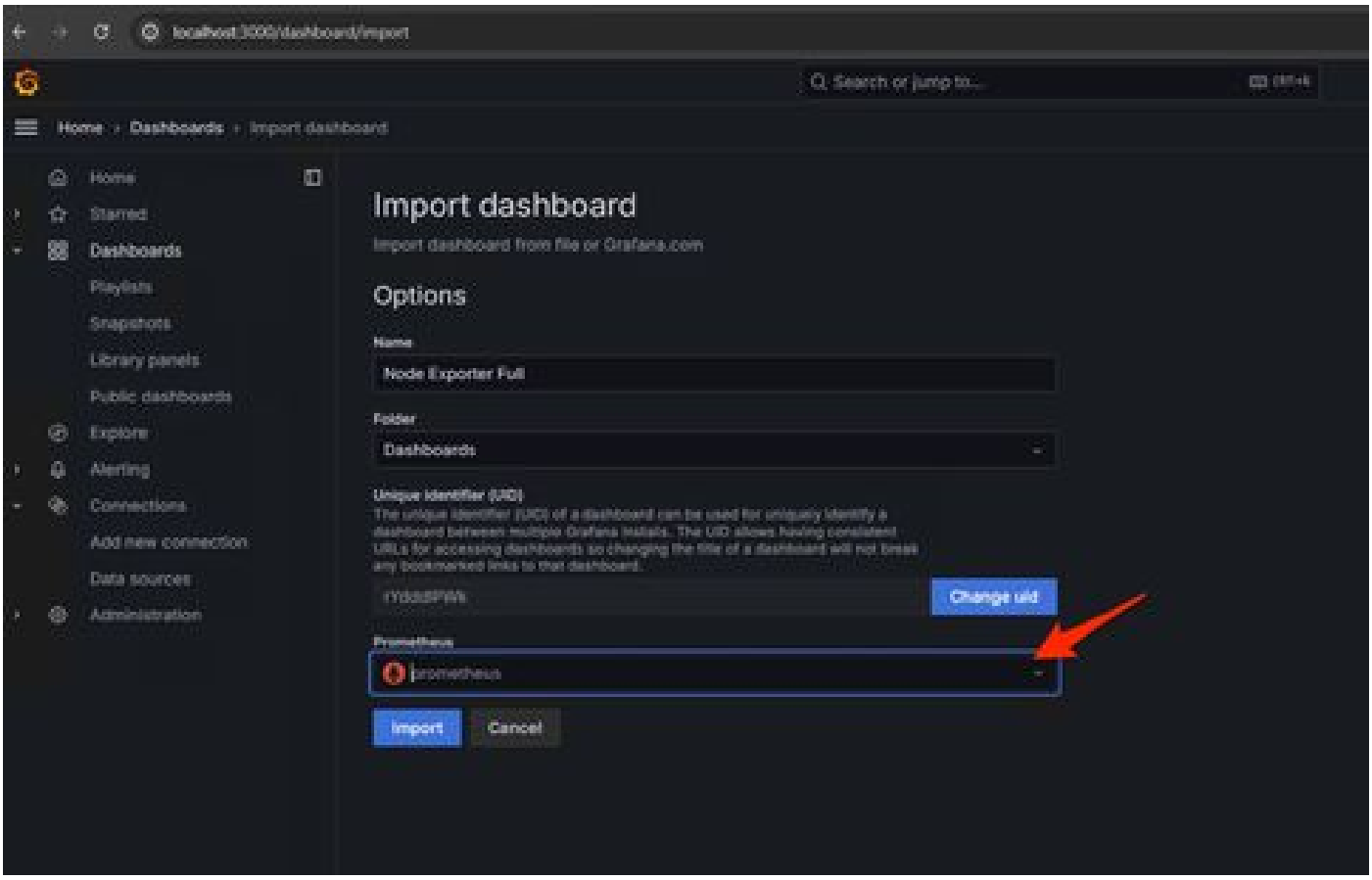
هناك العديد من قوالب لوحة معلومات Grafana متوفرة لمصدر العقد على موقع Grafana على الويب. أحدهما هو - مصدر العقدة مختلف

1. لاستيراد لوحة المعلومات هذه إلى مثيل Grafana تنزيل JSON، قم باستيراد ملف JSON في Grafana

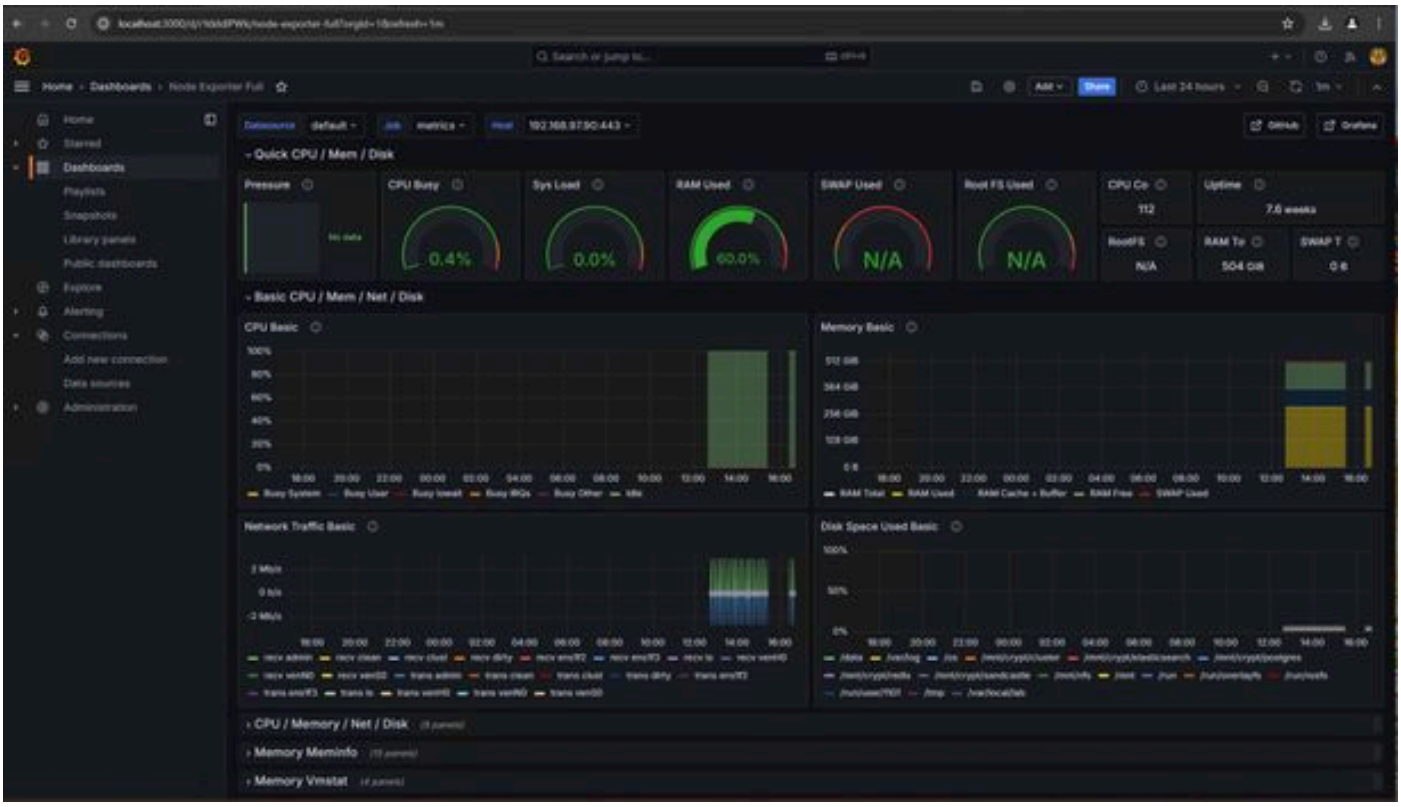


2. تحميل ملف JSON وتحديد مصدر Prometheusdata


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. سيؤدي ذلك إلى إنشاء لوحة معلومات بها الكثير من معلومات الأجهزة (لا تتوفر جميع مقاييس اللوحة)-



استكشاف الأخطاء وإصلاحها

- إذا فشل المشروع في الاتصال وسحب المقياس من جهاز SMA، ستركى الخطأ في الجلة < الأدوات

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

إذا كان هناك أي خطأ، فيجب إصلاح ذلك قبل أن يتمكن من سحب البيانات. المشكلة الشائعة هي أن شهادة SSL الخاصة بجهاز SMA Opadmin غير موثوق بها من قبل الجهاز المحلي. تأكد من إنشاء شهادة مسؤول SMA باستخدام IP و DNS SAN، وأضف المرجع المصدق الأساسي للتوقيع إلى مخزن ثقة الجهاز المحلي.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).