# Qualys で ISE 2.1 脅威中心型 NAC（TC-NAC）を設定する

## 目次



## 概要

このドキュメントでは、Identity Services Engine（ISE）2.1上で Threat-Centric NAC with Qualys を設定する方法を説明します。 Threat Centric Network Access Control（TC-NAC）機能を使用すると、許可ポリシーを、驚異および脆弱性アダプタから受け取る脅威と脆弱性の属性に基づいて作成することができます。

## 前提条件

### 要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco Identity Service Engine
- Qualys ScanGuard

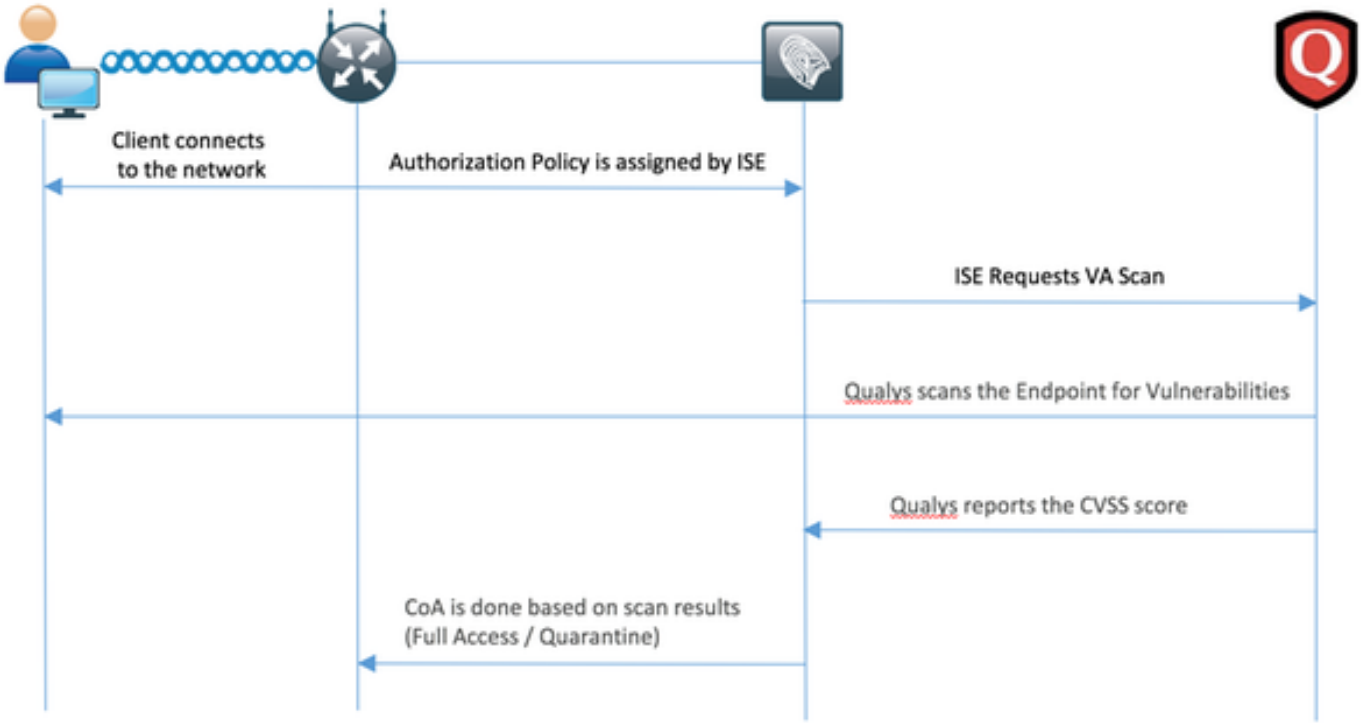
### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Service Engine バージョン 2.1
- ワイヤレス LAN コントローラ（WLC）8.0.121.0
- QualysGuard スキャナ 8.3.36-1、シグネチャ 2.3.364-2
- Windows 7 Service Pack 1

## 設定

### 高レベル フロー図




フローは次のとおりです。

1. クライアントがネットワークに接続すると、限定的なアクセスが付与され、[Assess Vulnerabilities] チェックボックスがオンになったプロファイルが割り当てられます。
2. PSN ノードが MNT ノードに Syslog メッセージを送信し、許可が行われたことと、VA スキャンが許可ポリシーの結果であることを確認します。
3. MNT ノードは、次のデータを使用して、TC-NAC ノードに（Admin WebApp を使用して）SCAN を送信します。
   - MAC Address
   - IP アドレス
   - スキャン間隔
   - 有効化されている定期的なスキャン
   - 発信元 PSN
4. Qualys TC-NAC（Docker コンテナにカプセル化されています）は、Qualys クラウドと（REST API 経由で）通信し、必要に応じてスキャンをトリガーします。

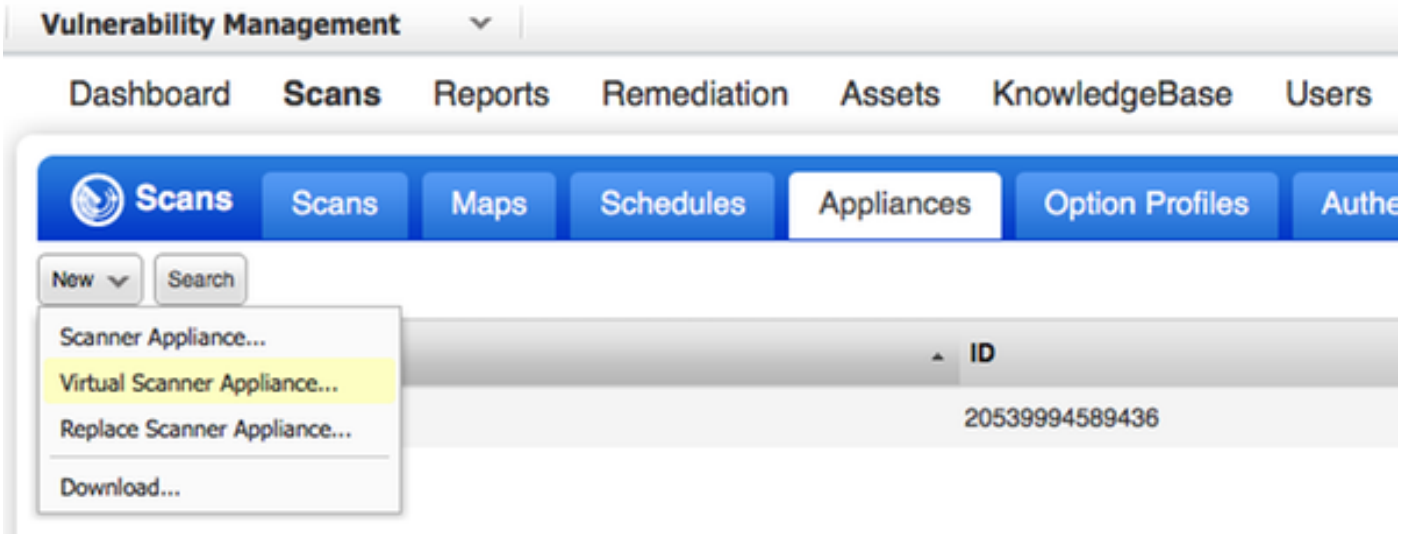
5. Qualys クラウドは、エンドポイントをスキャンするよう Qualys スキャナに指示します。
6. Qualys スキャナは、スキャンの結果を Qualys クラウドに送信します。
7. 次のスキャン結果が TC-NAC に返送されます。
   - MAC Address
   - すべての CVSS スコア
   - すべての脆弱性（QID、タイトル、CVEID）
8. TC-NAC は、ステップ 7 のすべてのデータを PAN に反映します。
9. 設定されている許可ポリシーに従い、必要に応じて CoA がトリガーされます。

## Qualys クラウドとスキャナの設定

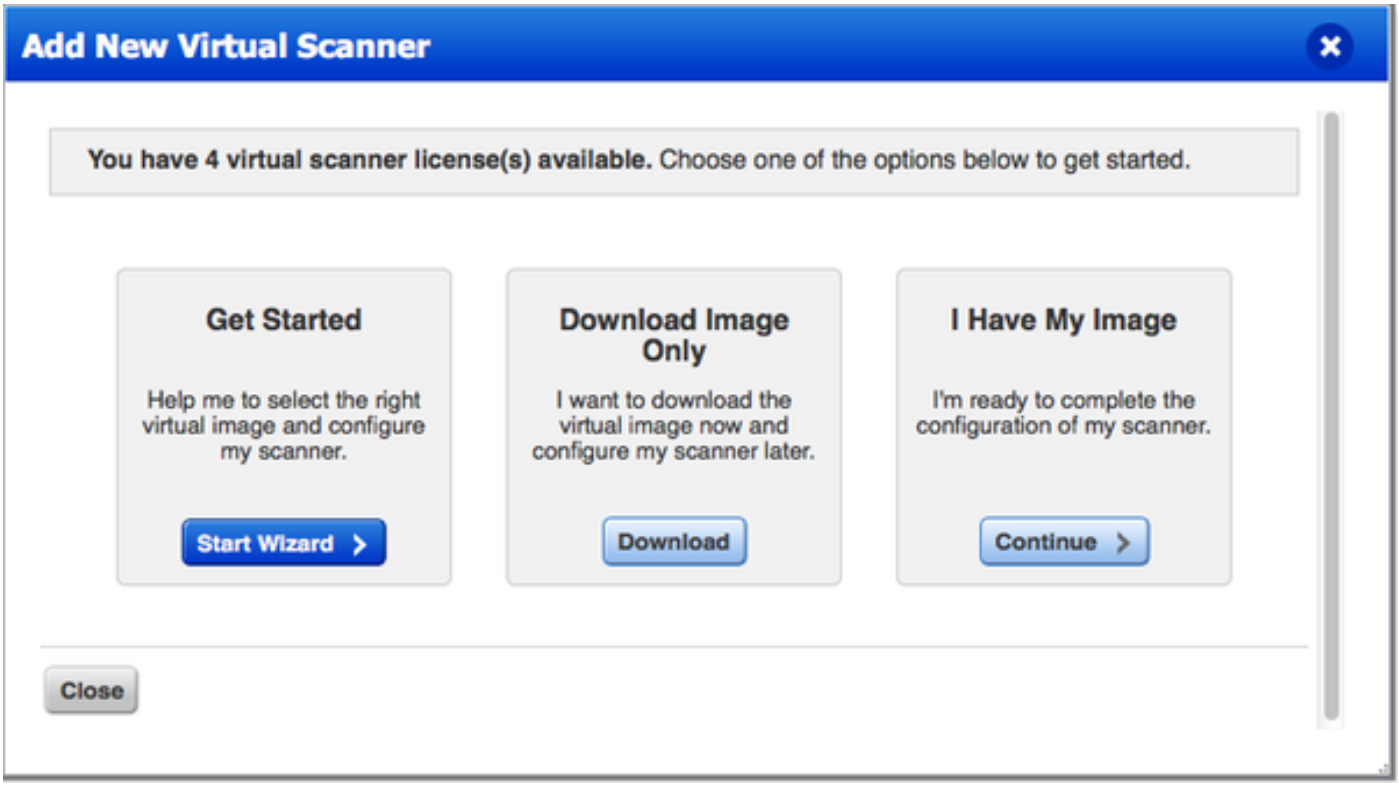
> **注意**： このドキュメントに記載する Qualys の設定は、ラボの目的のために行うものです。設計上の考慮事項については、Qualys エンジニアに相談してください。

### ステップ 1：Qualys スキャナの導入

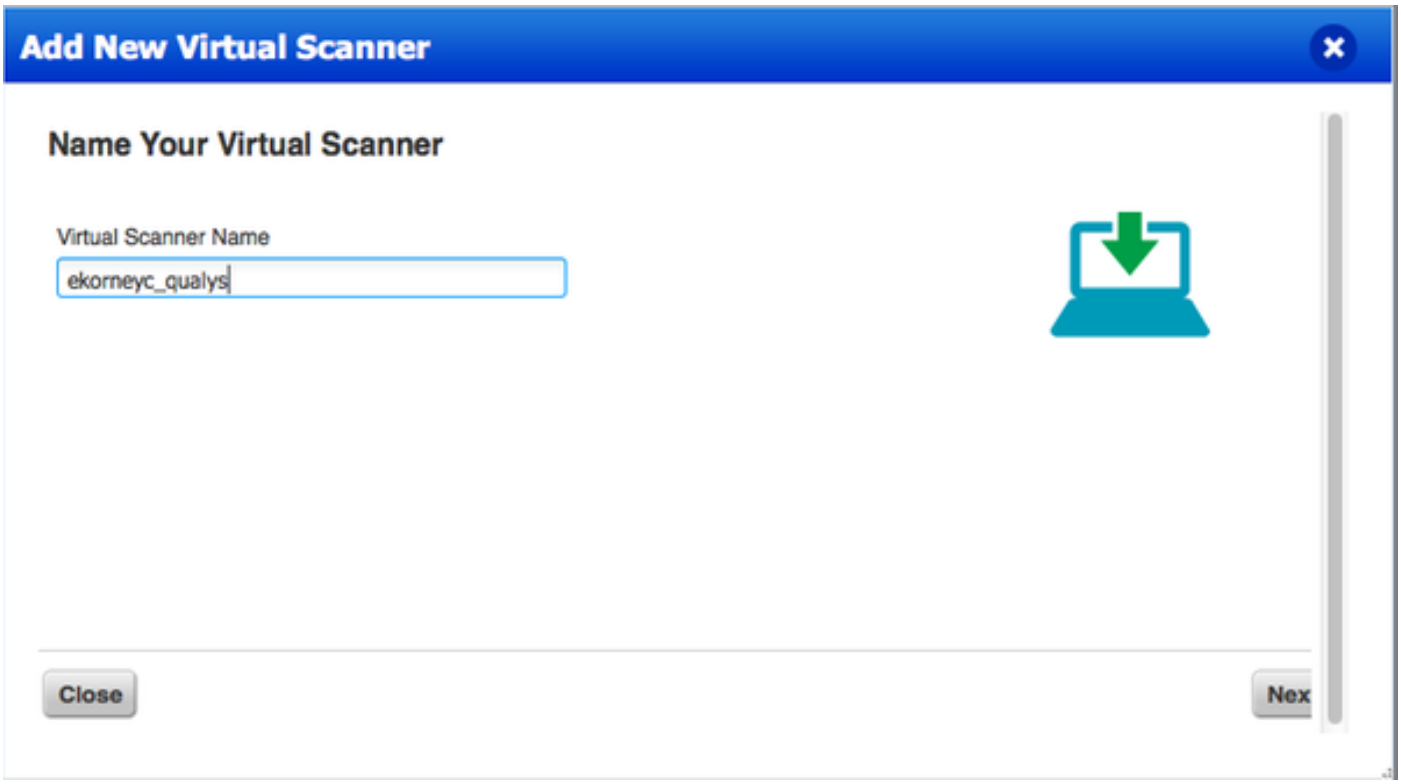
Qualys スキャナは OVA ファイルから導入できます。 Qualys クラウドにログインし、[Scans] > [Appliances and select New] > [Virtual Scanner Appliance] の順に移動します。




[Download Image Only] を選択し、適切な配布方法を選択します。




[Scans] > [Appliances and select New] > [Virtual Scanner Appliance] に移動して [I Have My Image] を選択し、アクティベーション コードを取得します。




スキャナ名を入力すると、後で使用する認証コードが付与されます。

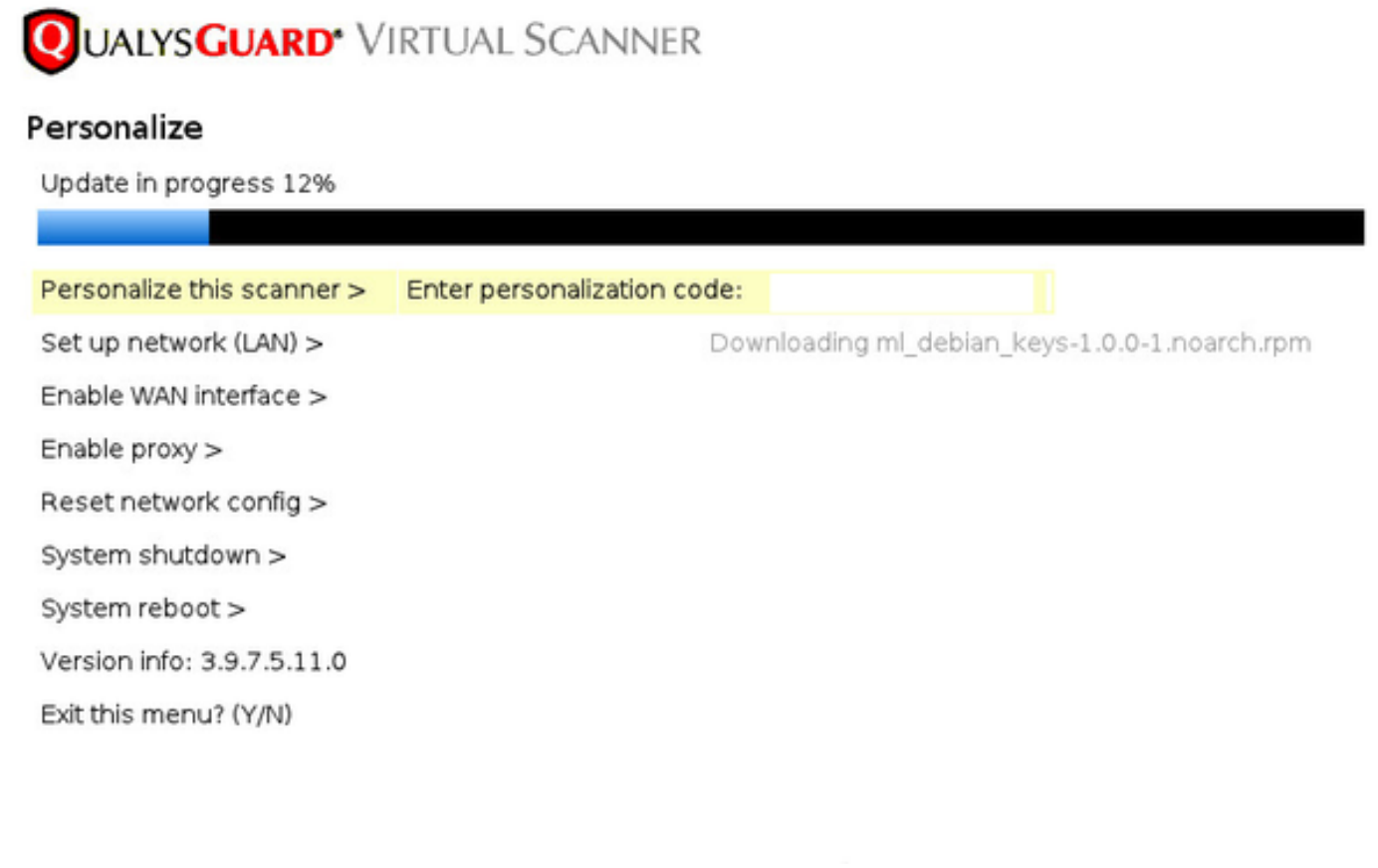
**手順 2：Qualys スキャナの設定**

OVA を選択した仮想化プラットフォームに展開します。 完了したら、次の設定を行います。

- ネットワーク（LAN）のセットアップ

- WAN インターフェイスの設定（2 つのインターフェイスを使用する場合）
- プロキシの設定（プロキシを使用する場合）
- スキャナのパーソナライズ


その後、スキャナが Qualys に接続され、最新のソフトウェアとシグネチャがダウンロードされます。




スキャナが接続されているか確認するには、[Scans] > [Appliances] に移動します。

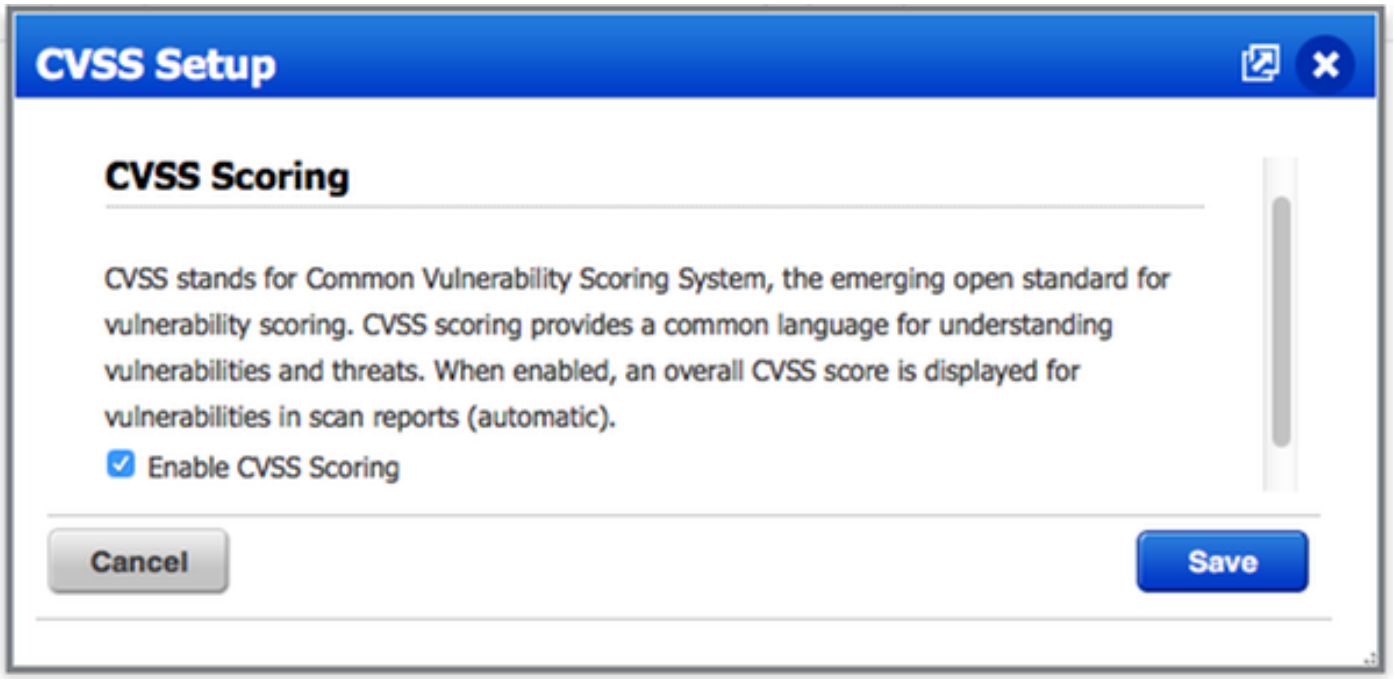
左側に緑色の接続中サインが表示されていれば、スキャナの準備は整っています。LAN IP、WAN IP、スキャナのバージョン、およびシグネチャも表示されています。

## ISE の設定

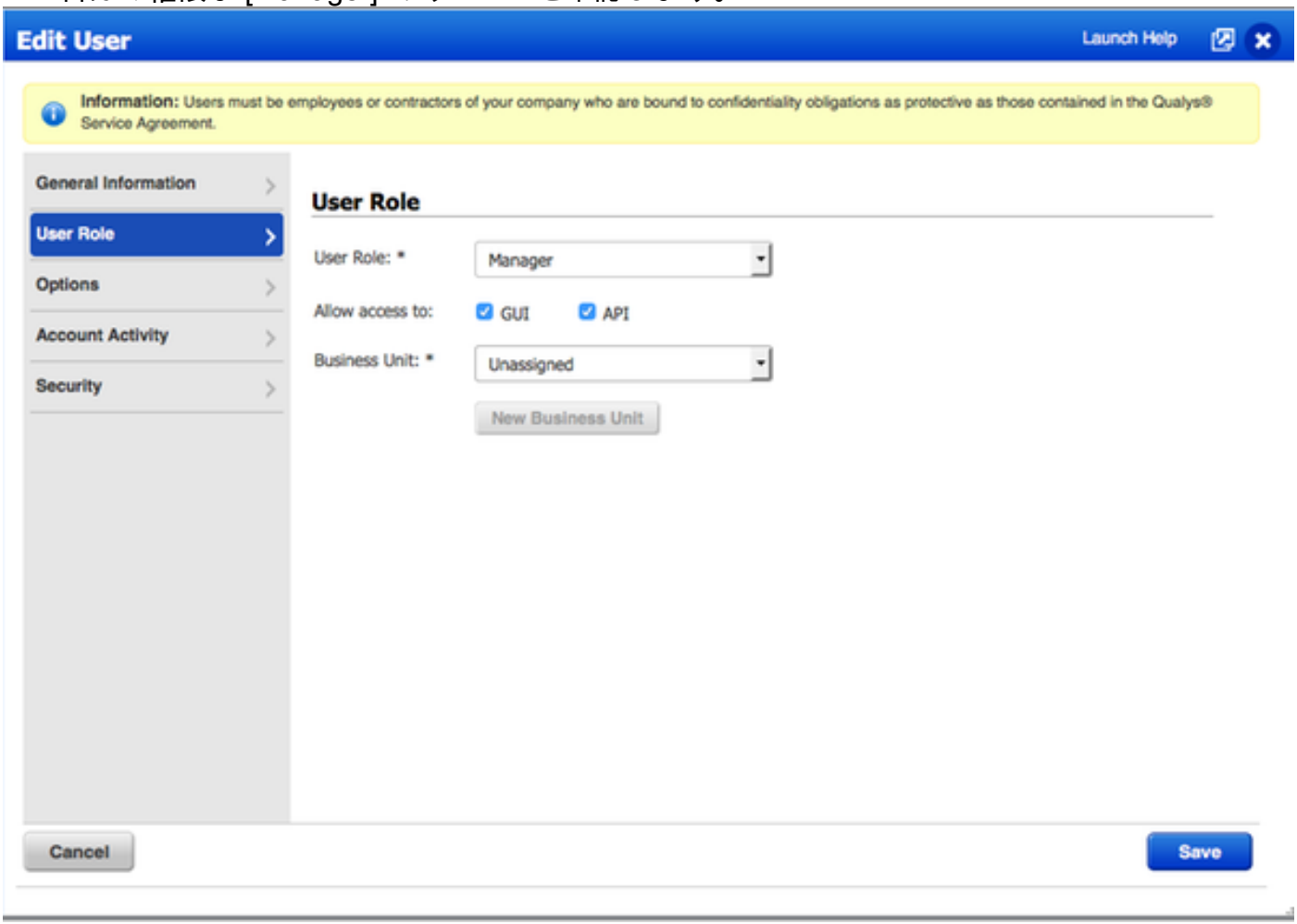
Qualys スキャナと Qualys クラウドの設定が完了していても、ISE との統合が問題なく機能するようにするには、クラウドの設定を調整する必要があります。 この作業は、GUI を使用してアダプタを設定する前に行ってください。理由は、CVSS スコアを含むナレッジ ベースは、アダプタの初回設定の後にダウンロードされるためです。

### ステップ 1：ISE との統合のための Qualys クラウドの調整

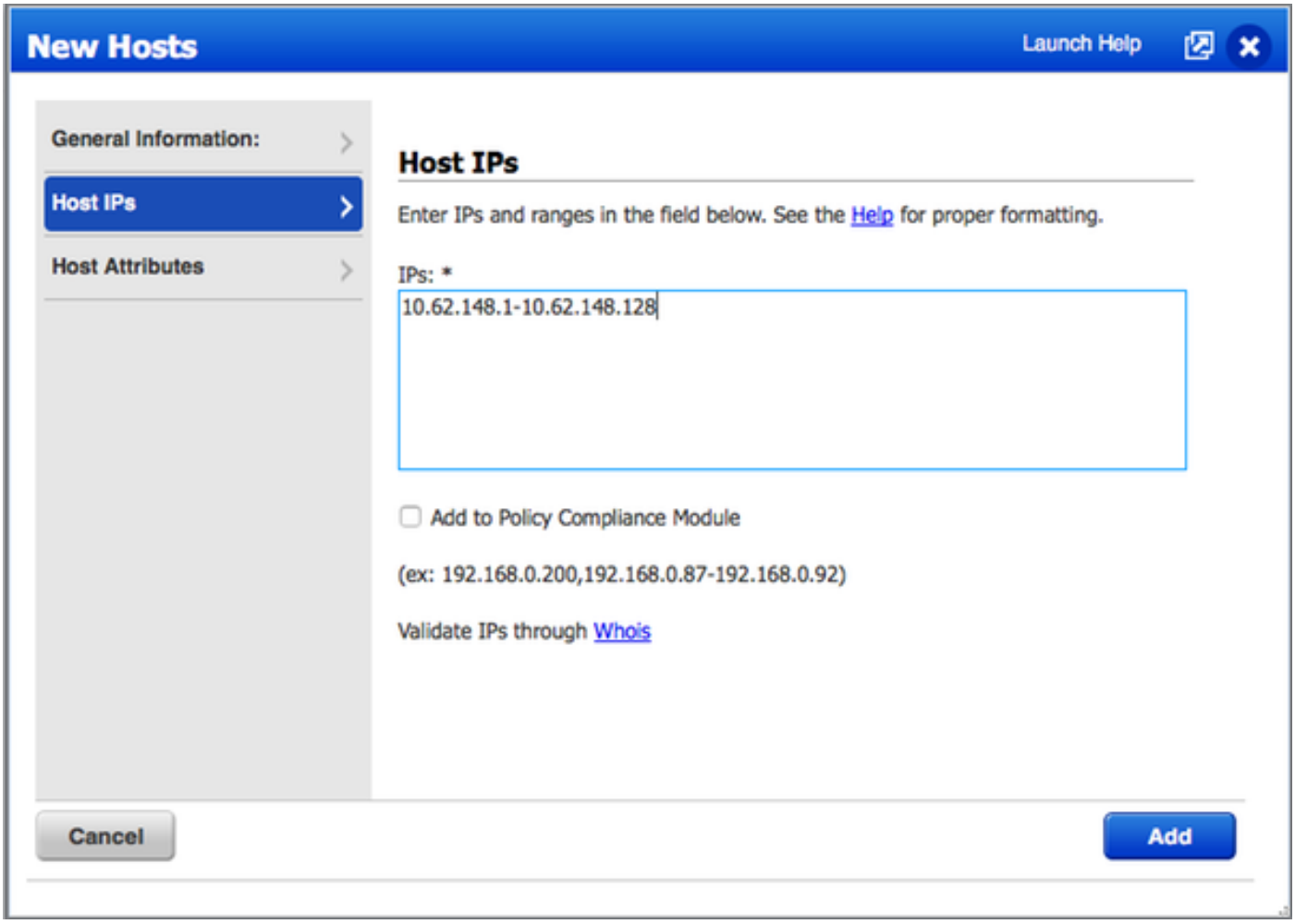
- [Vulnerability Management] > [Reports] > [Setup] > [CVSS] > [Enable CVSS Scoring] の順に選択し、CVSS スコアを有効にします。




- アダプタ設定で使用するユーザ クレデンシャルに管理者権限があることを確認します。 左上の角から自分のユーザを選択し、[User Profile] をクリックします。 [User Role] に表示される自分の権限が [Manager] であることを確認します。



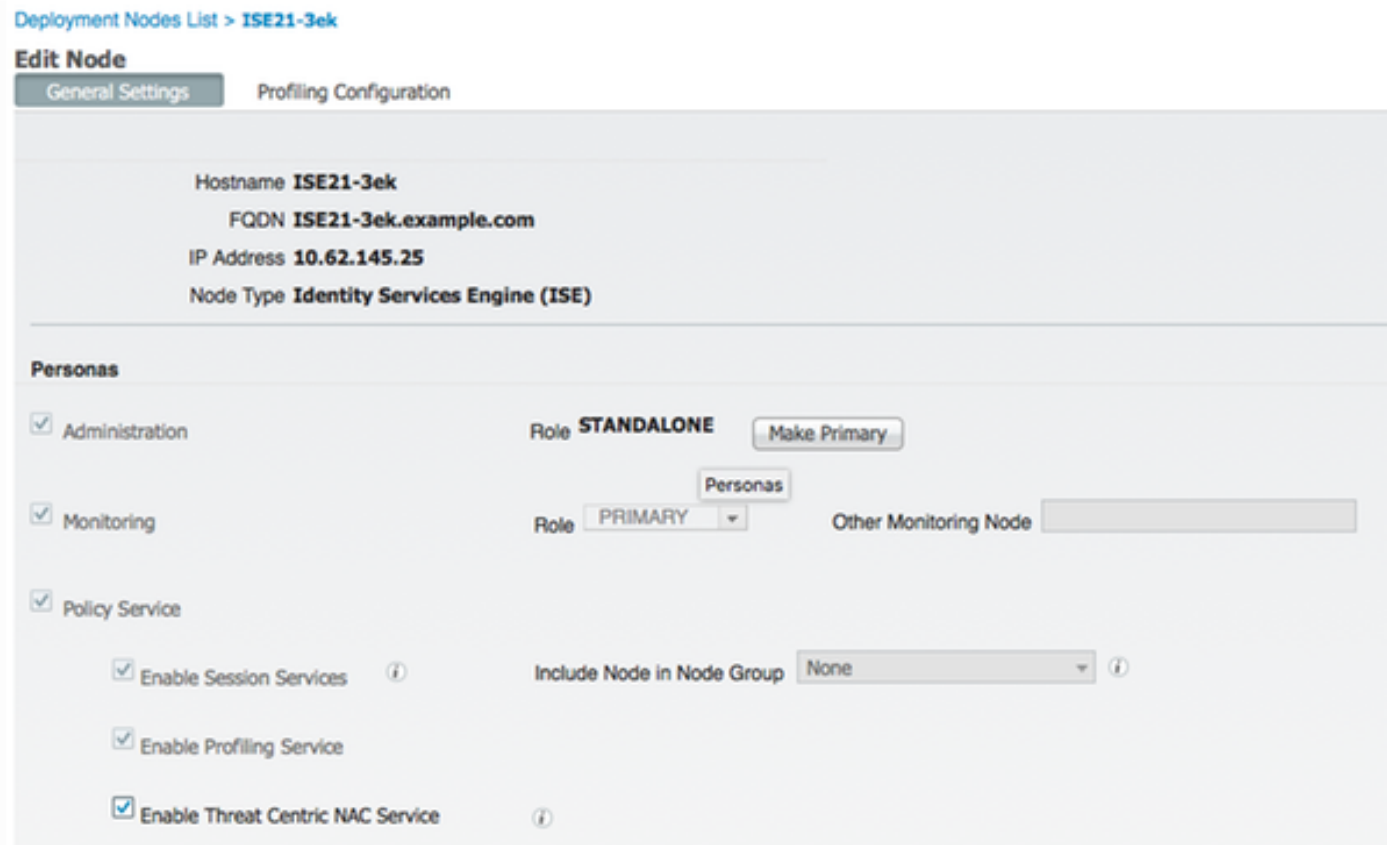

- [Vulnerability Management] > [Assets] > [Host Assets] > [New] > [IP Tracked Hosts] で、脆弱性評価を必要とするエンドポイントの IP アドレス/サブネットが Qualys に追加されていることを確認します。




### 手順 2：TC-NAC サービスの有効化

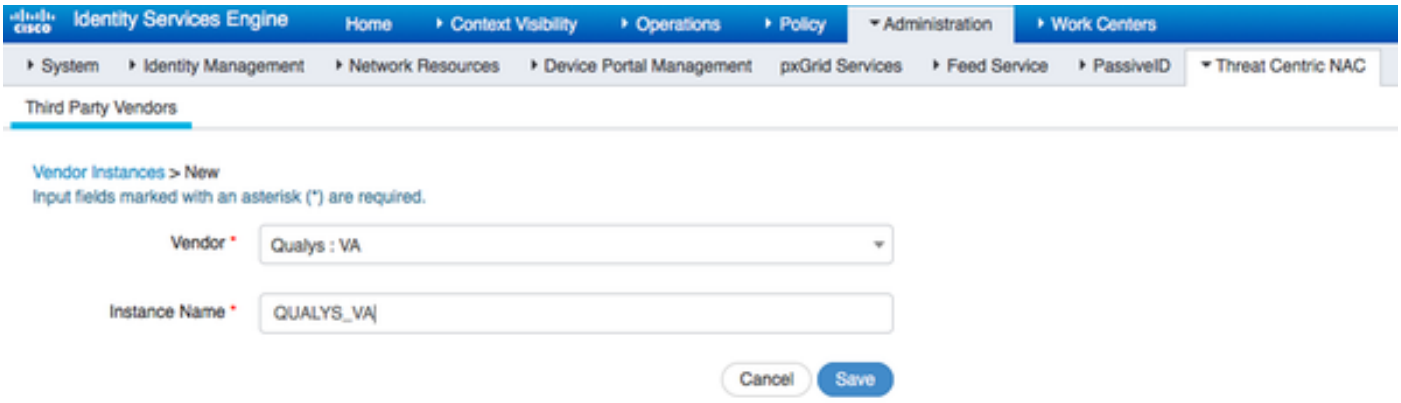
[Administration] > [Deployment] > [Edit Node] で、TC-NAC サービスを有効化します。 チェック [Enable Threat Centric NAC Service ] チェックボックスにマークを付けます。

> **注:** TC-NAC ノードは、導入ごとに 1 つだけ存在します。

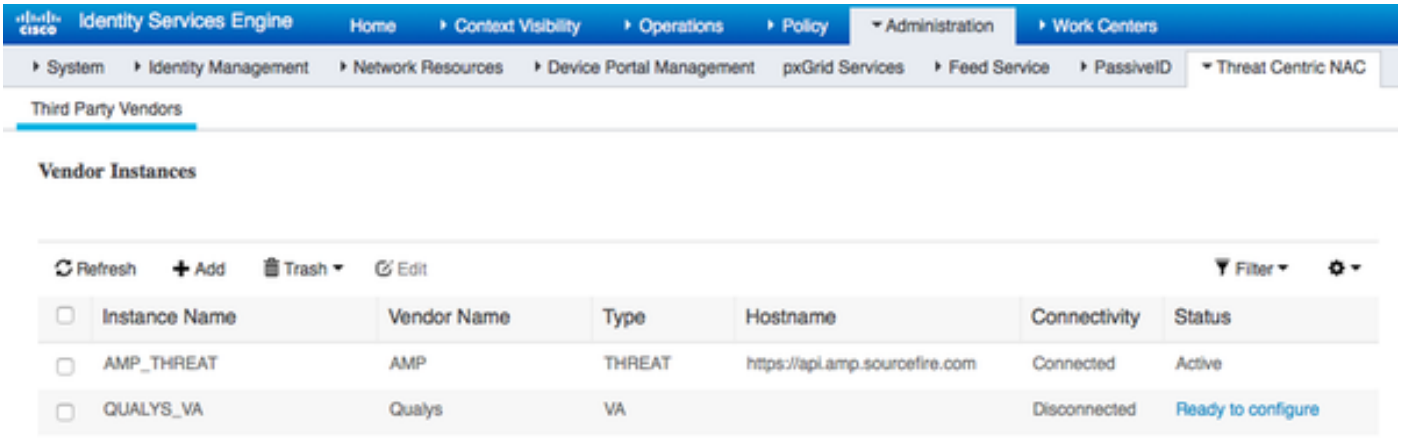



### 手順 3：Qualys アダプタの ISE VA フレームワークへの接続の設定

[Administration] > [Threat Centric NAC] > [Third Party Vendors] > [Add] の順に移動します。[Save] をクリックします。

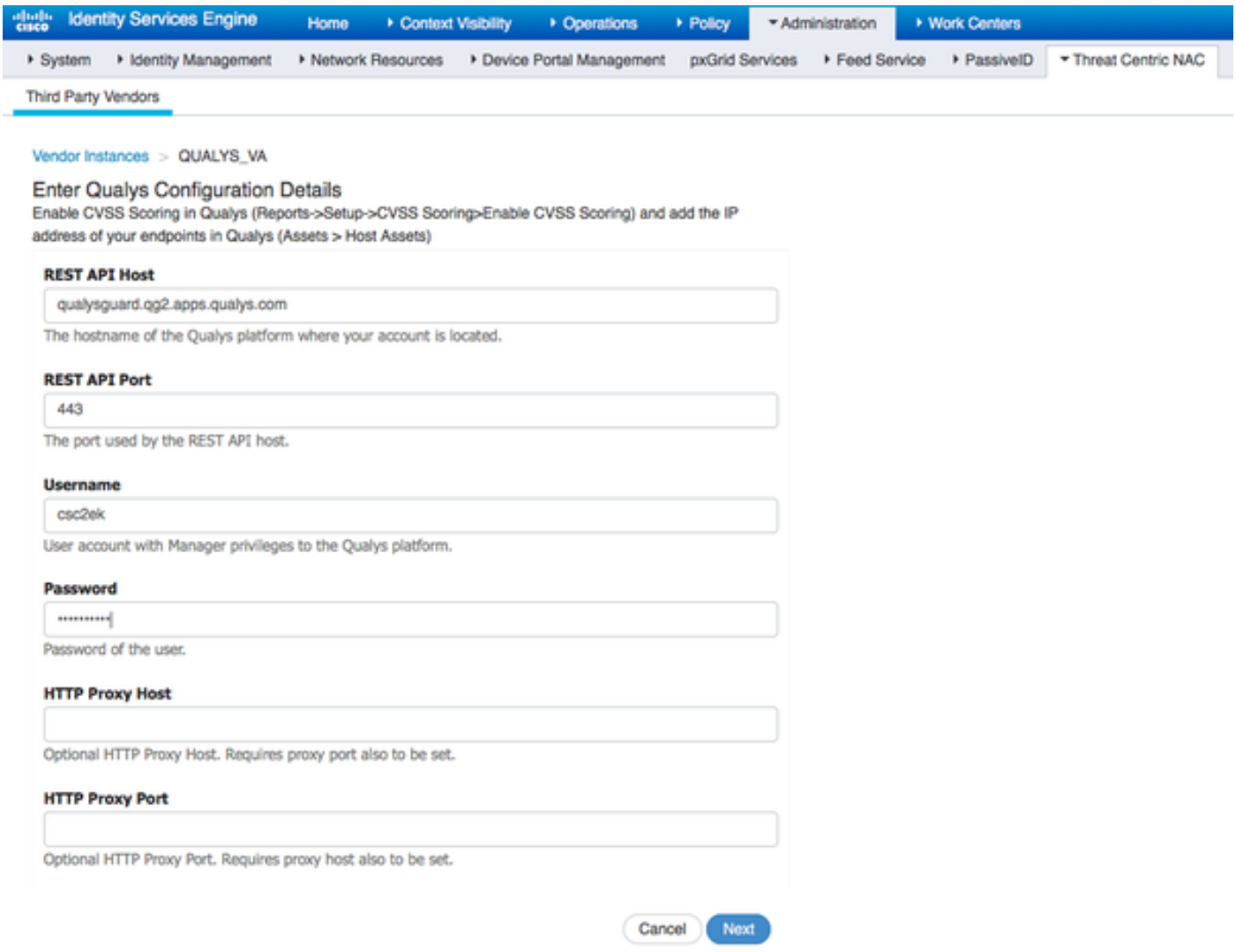



Qualys インスタンスが [Ready to configure] 状態に遷移したら、[Status] 列で [Ready to configure] オプションをクリックします。

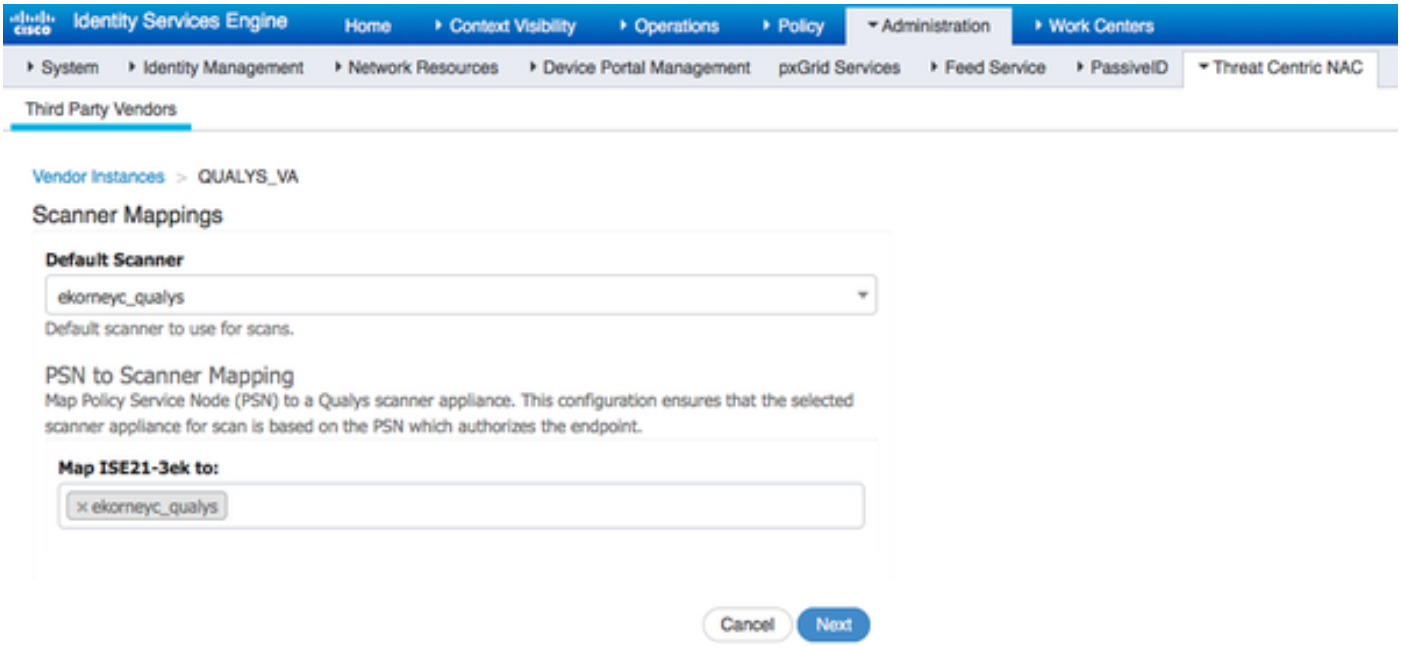



[REST API Host] には、Qualys クラウドに使用する、自分のアカウントがあるホストを設定します。 この例では、「qualysguard.qg2.apps.qualys.com」が設定されています。

アカウントに管理者権限があることを確認し、[Next] をクリックします。

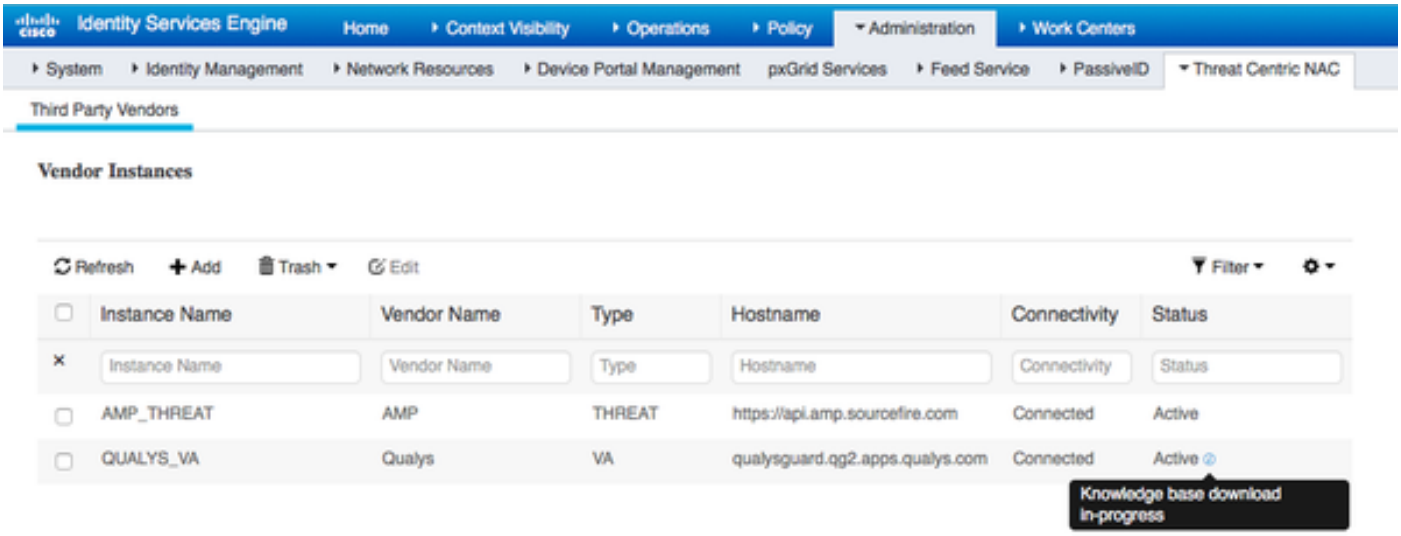



ISE により、Qualys クラウドに接続されているスキャナに関する情報がダウンロードされます。このページでは、PSN to Scanner Mapping を設定することができます。 この設定により、エンドポイントを承認する PSN に基づいてスキャナが選択されるようにできます。




詳細設定については、『ISE 2.1 管理者ガイド』を参照してください。このガイドへのリンクは、このドキュメントの「参照」の項に記載されています。 [Next] と [Finish] をクリックします。 Qualys インスタンスが [Active] 状態になり、ナレッジ ベースのダウンロードが開始します。

**注:** Qualys インスタンスは、導入ごとに 1 つだけ存在します。



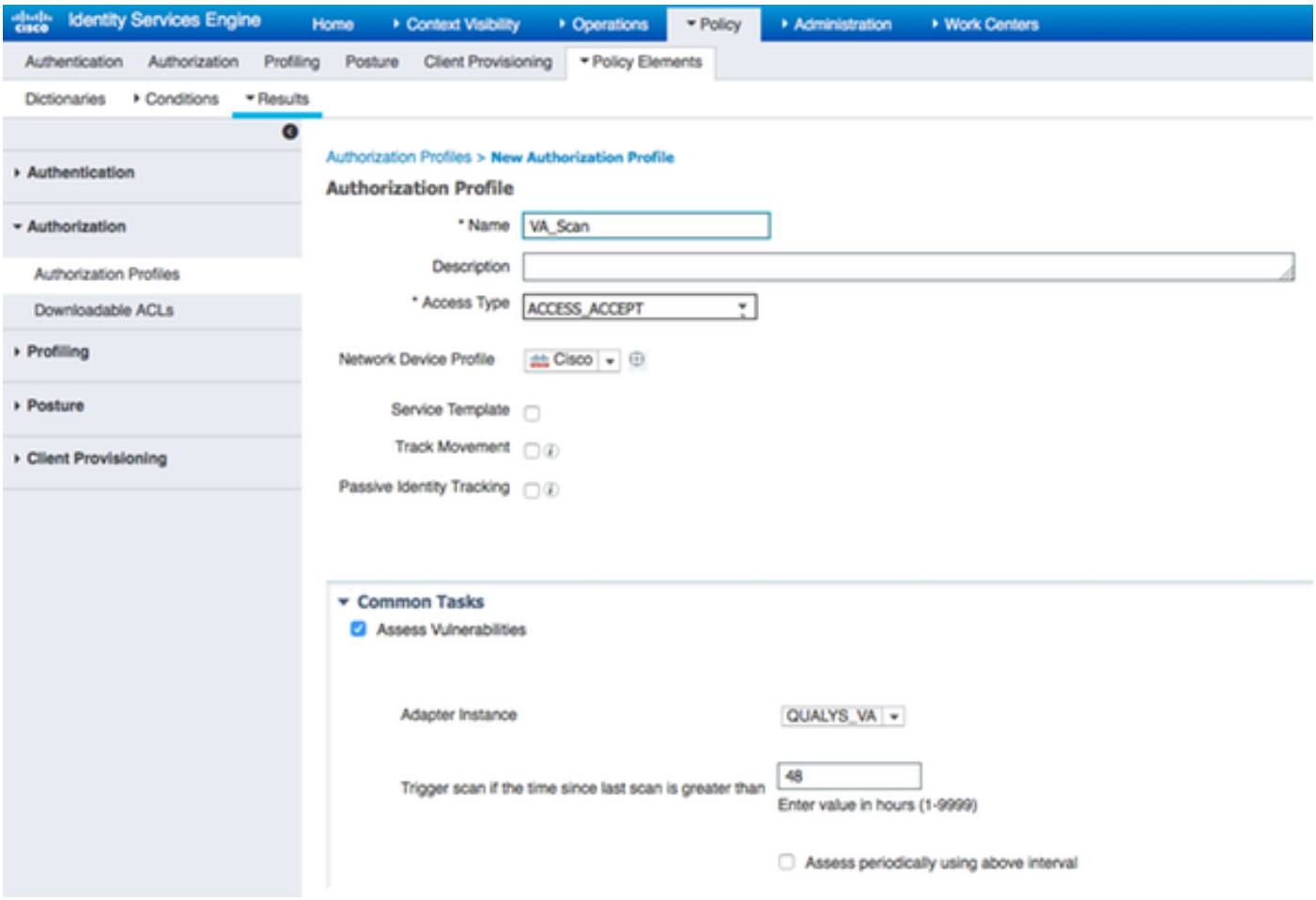

### 手順 4：VA スキャンをトリガーするための許可プロファイルの設定

[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。新しいプロファイルを追加します。 [Common Tasks] で、[Vulnerability Assessment] チェックボックスをオンにします。
オンデマンドのスキャン間隔は、ネットワーク設計に従って選択します。

許可プロファイルには、次の AV ペアが含まれています。

cisco-av-pair = on-demand-scan-interval=48
cisco-av-pair = periodic-scan-enabled=0
cisco-av-pair = va-adapter-instance=796440b7-09b5-4f3b-b611-199fb81a4b99

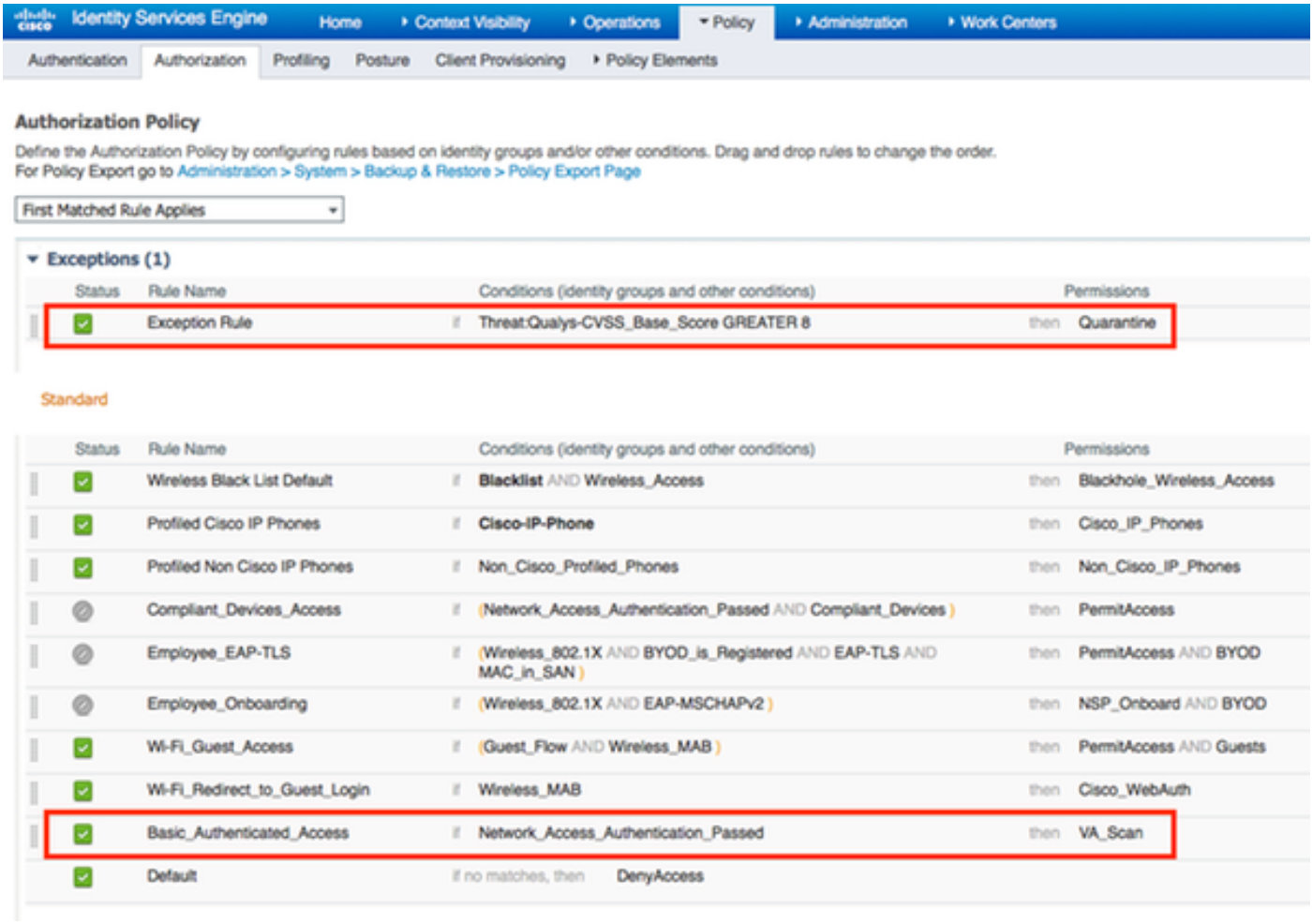
これらは、Access-Accept パケットでネットワーク デバイスに送信されます。ただし、これらの実際の目的は、MNT ノードにスキャンのトリガーが必要になったことを通知することです。MNT は、TC-NAC ノードに Qualys クラウドと通信するよう指示します。




### ステップ 5：許可ポリシーの設定

- ステップ 4 で設定した新しい許可プロファイルが使用されるよう、許可ポリシーを設定します。[Policy] > [Authorization] > [Authorization Policy] に移動し、[Basic_Authenticated_Access] ルールを選択し、[Edit] をクリックします。 [Permissions] を、[PermitAccess] から新しく作成した [Standard VA_Scan] に変更します。 これにより、脆弱性スキャンが全ユーザに対して実行されるようになります。 [Save] をクリックします。

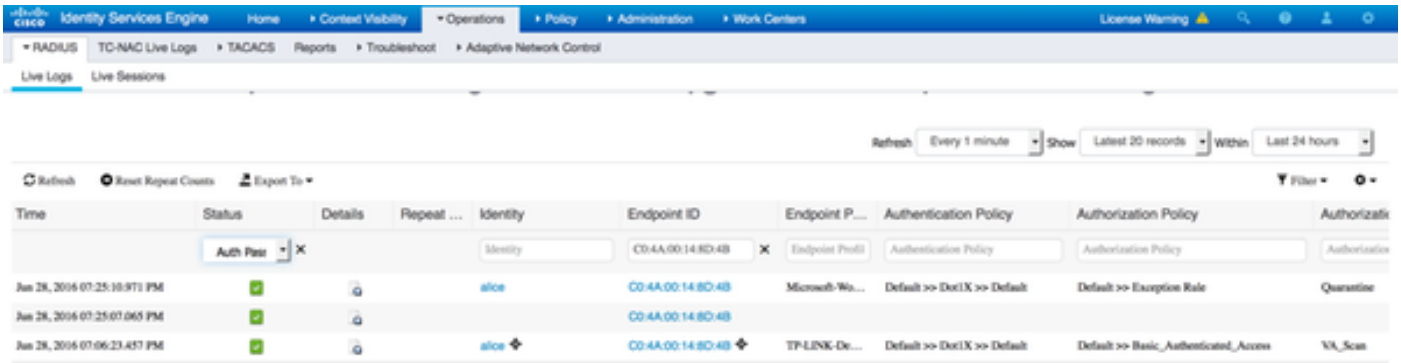
- 検疫マシンの許可ポリシーを作成します。 [Navigate to Policy] > [Authorization] > [Authorization Policy] > [Exceptions] に移動し、[Exception Rule] を作成します。 [Conditions] > [Create New Condition (Advanced Option)] > [Select Attribute] をクリックし、画面を下へスクロールして [Threat] をクリックします。 [Threat] 属性を展開し、[Qualys-CVSS_Base_Score] を選択します。 演算子を [Greater Than] に変更し、セキュリティ ポリシーに従って値を入力します。 許可プロファイル [Quarantine] では、脆弱なマシンには限定的なアクセスが付与されるようにする必要があります。



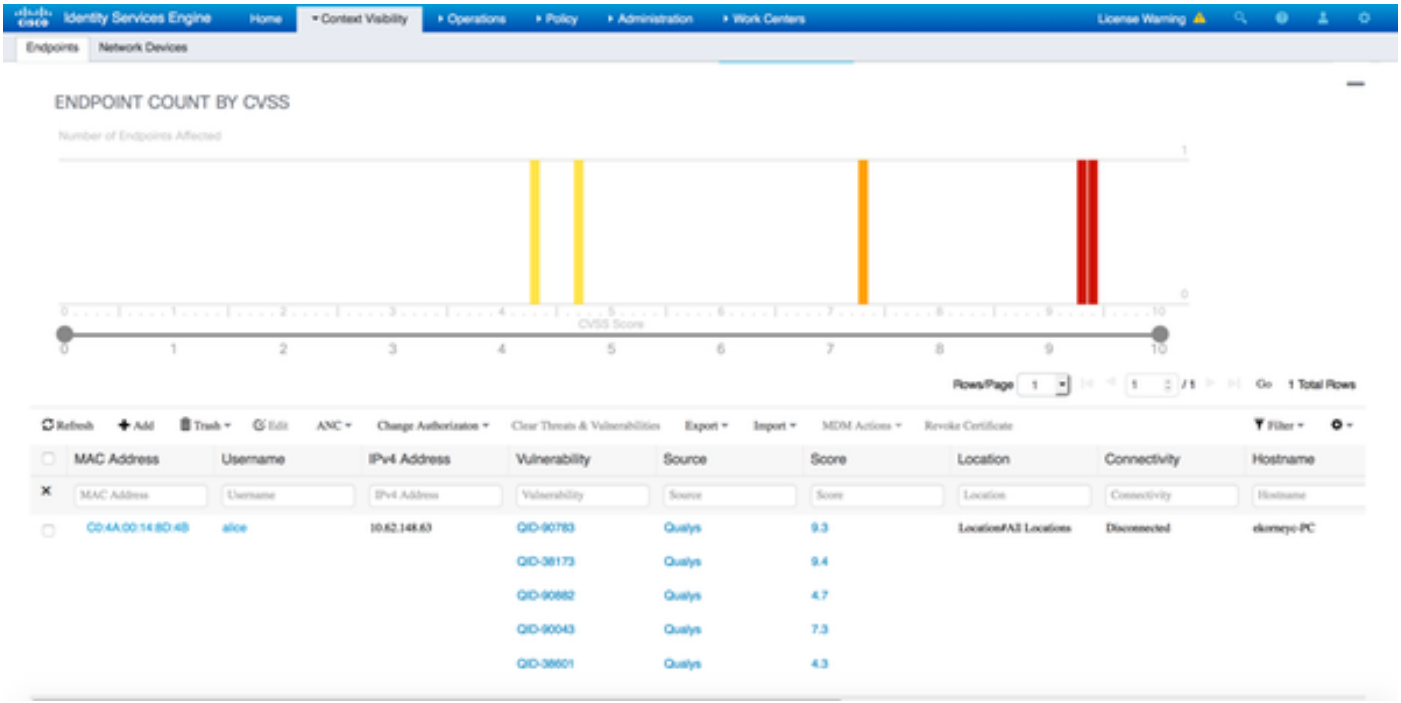

# 確認

## Identity Services Engine

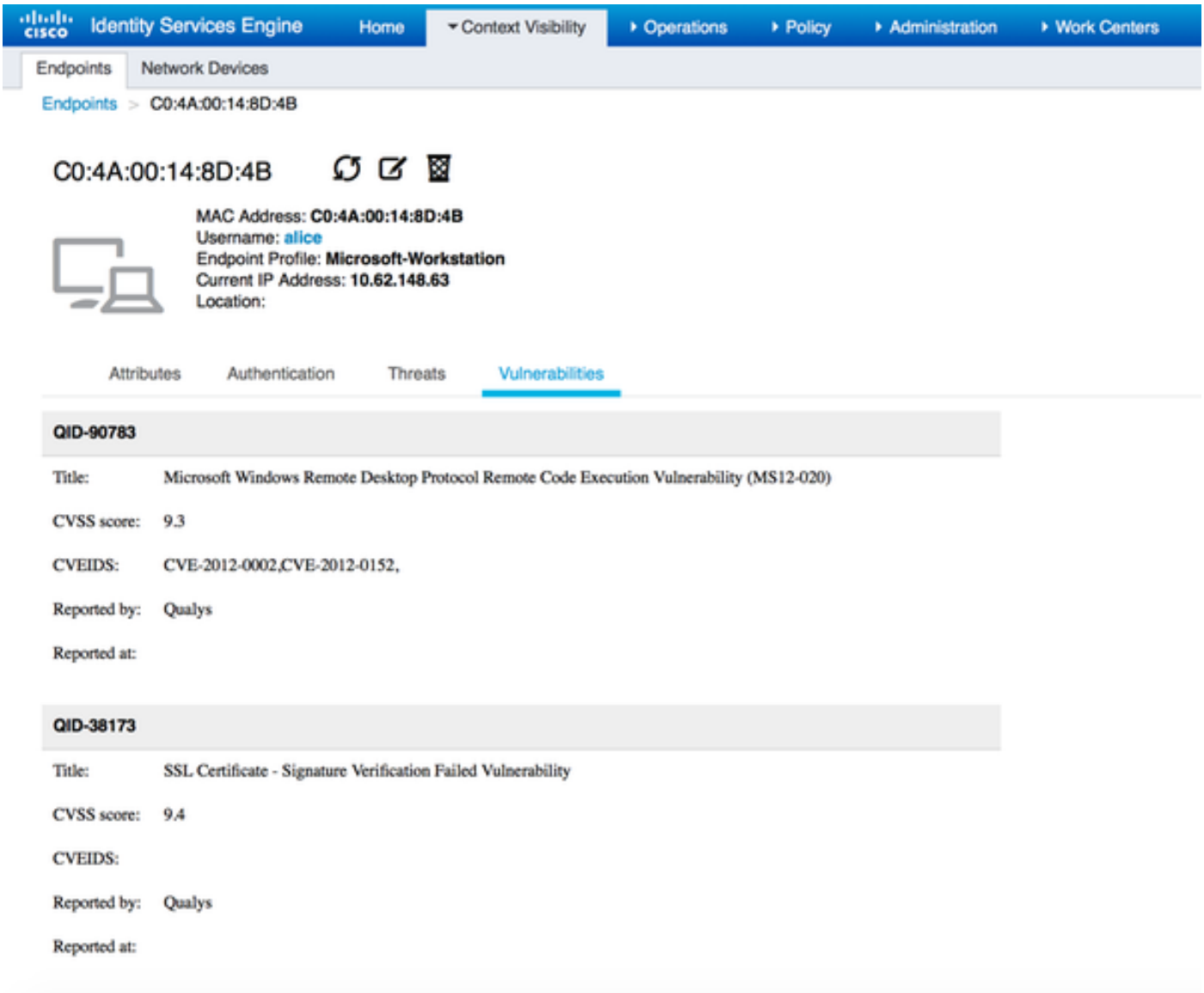
初回の接続により、VA スキャンがトリガーされます。 スキャンが終了すると CoA 再認証がトリガーされ、新しいポリシーが、一致していれば適用されます。




どの脆弱性が検出されたか確認するには、[Context Visibility] > [Endpoints] に移動します。 各エンドポイントの脆弱性を Qualys が与えたスコアで確認します。



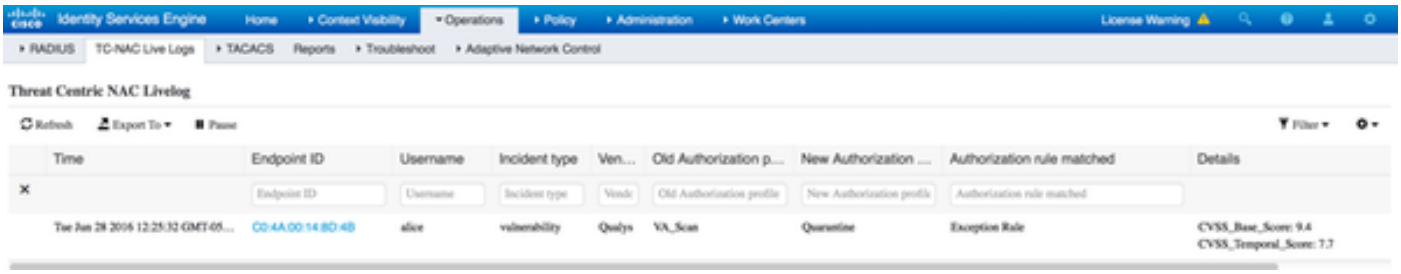

特定のエンドポイントを選択すると、[Title] や [CVEIDS] など、各脆弱性の詳細が表示されます。




[Operations] > [TC-NAC Live Logs] では、適用された新旧の許可ポリシーと CVSS_Base_Score

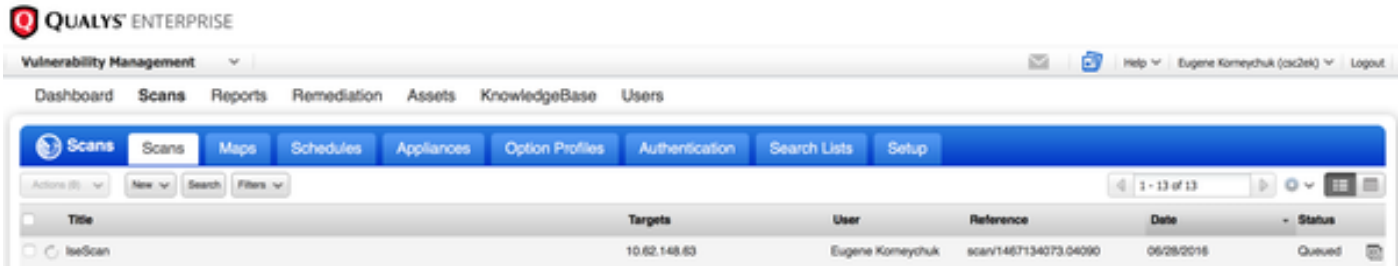
の詳細が確認できます。

> **注:** 許可条件は、CVSS_Base_Score に基づいて設定されます。CVSS_Base_Score は、エンドポイントについて検出された最大の脆弱性スコアと同じ値です。

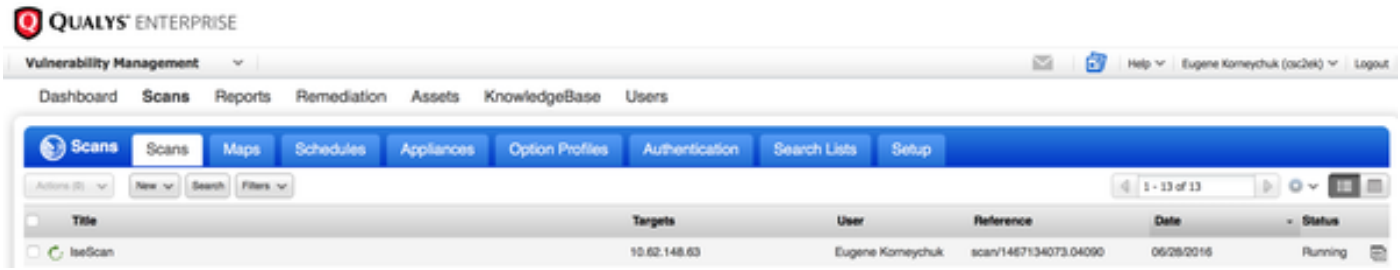



## Qualys クラウド

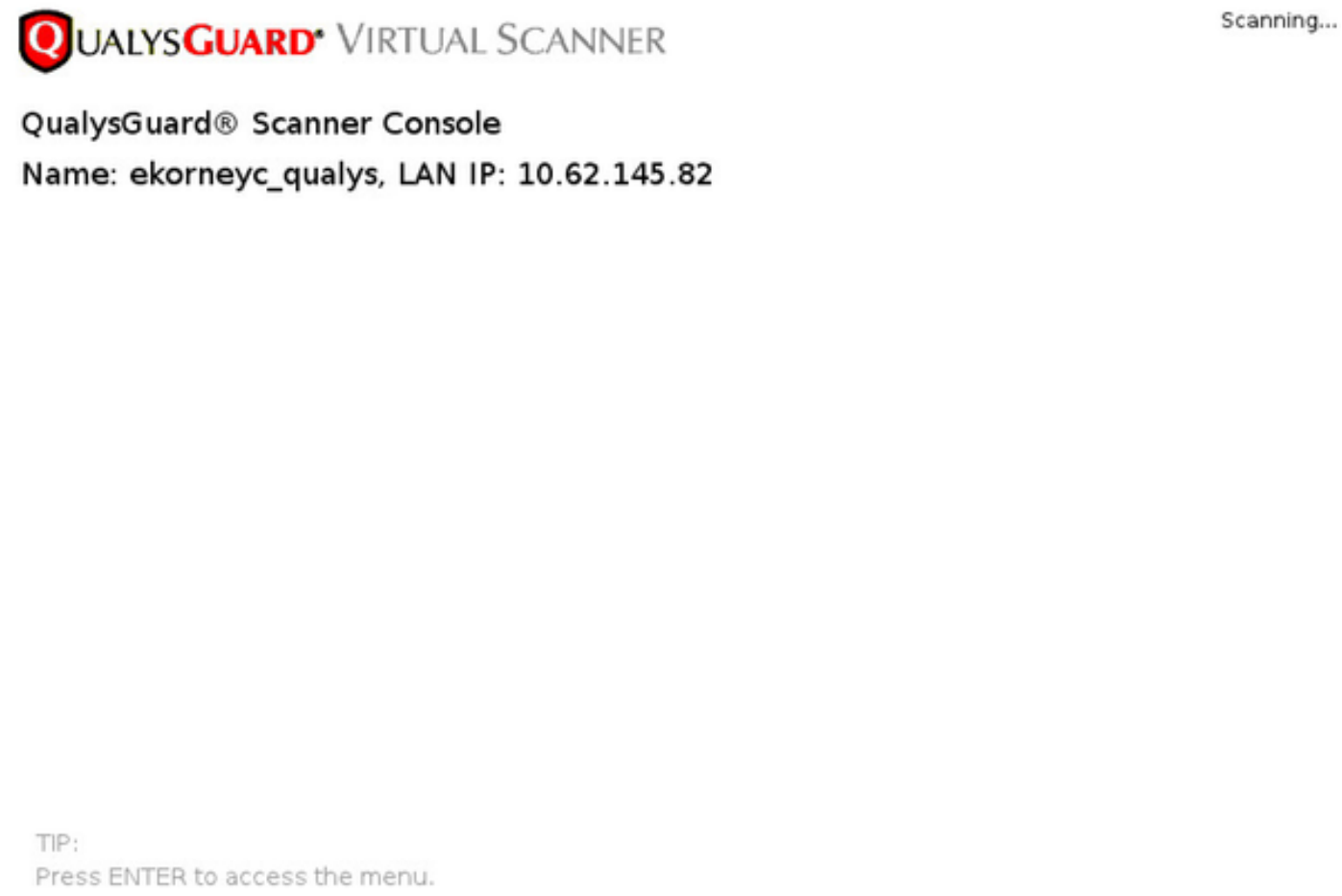
VA スキャンが TC-NAC でトリガーされると、Qualys はスキャンをキューに入れます。これは [Scans] > [Scans] で確認できます。



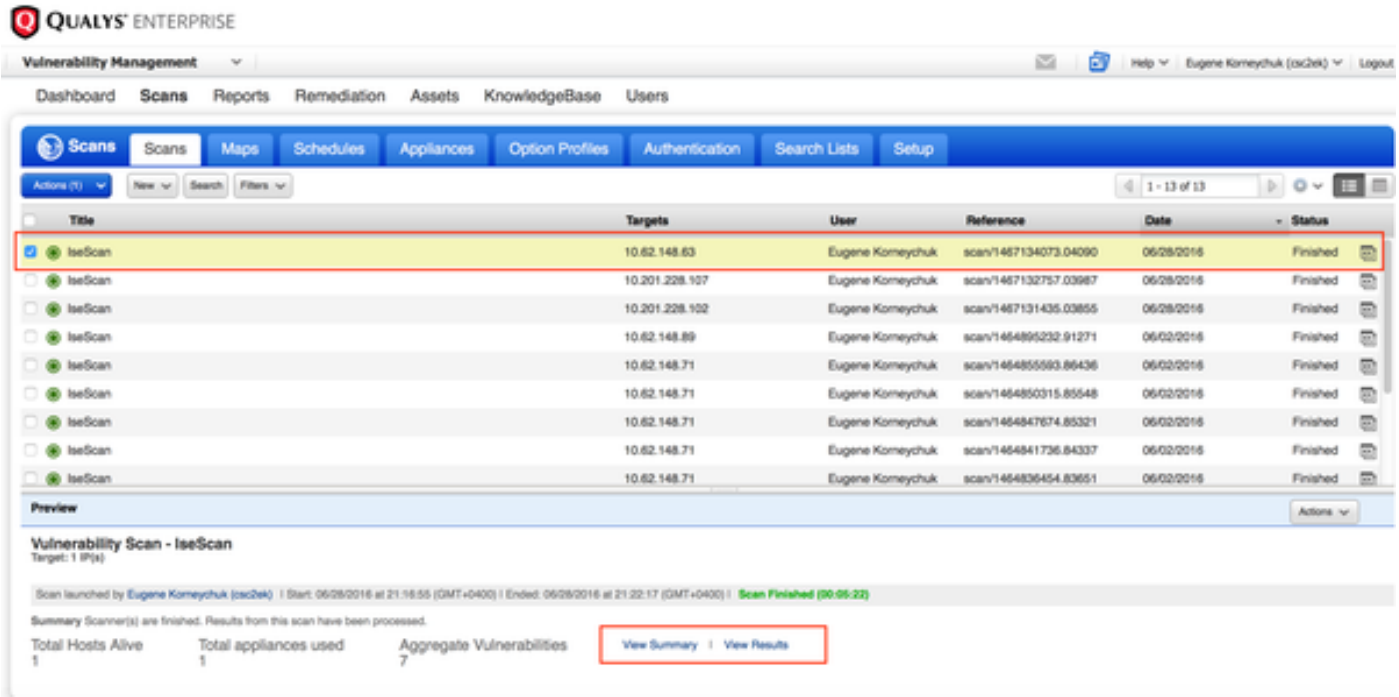

その後、状態が [Running] に遷移します。これは、Qualys クラウドが Qualys スキャナに実際のスキャンを実行するよう指示したことを意味します。



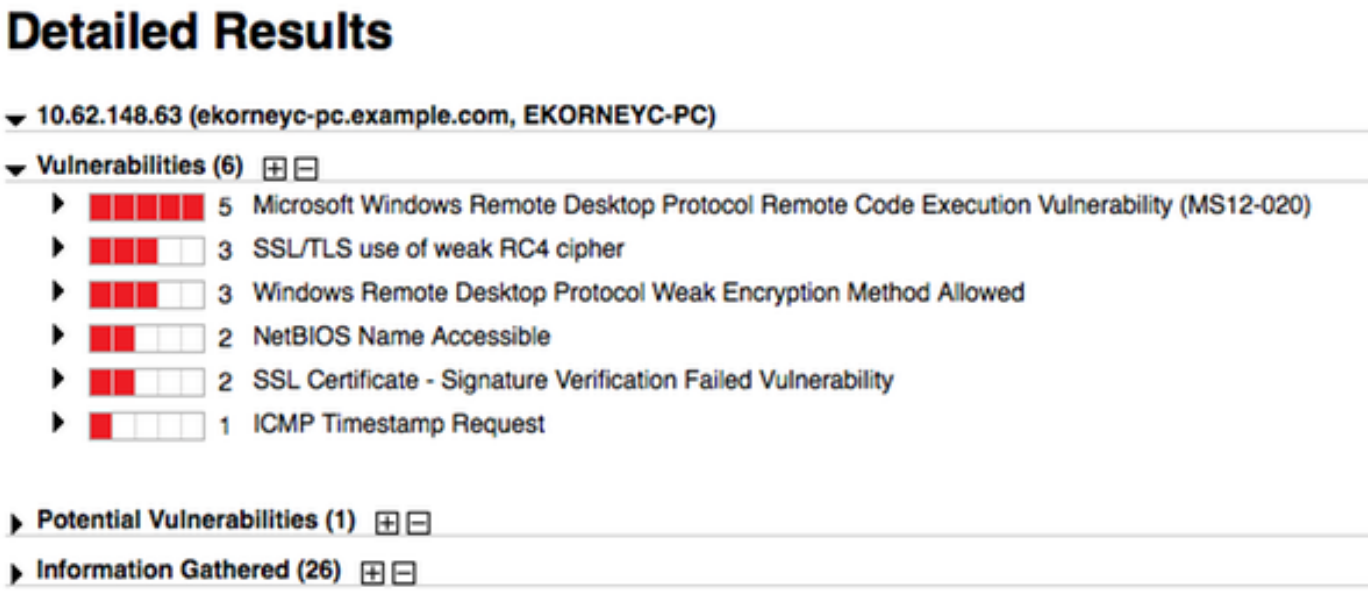

スキャナによるスキャンの実行中は、[Scanning...] という サインが QualysGuard の右上の隅に表示されます。




スキャンが完了すると、[Finished] 状態に遷移します。 結果を表示するには、[Scans] > [Scans] で必要なスキャンを選択して、[View Summary] または [View Results] をクリックします。



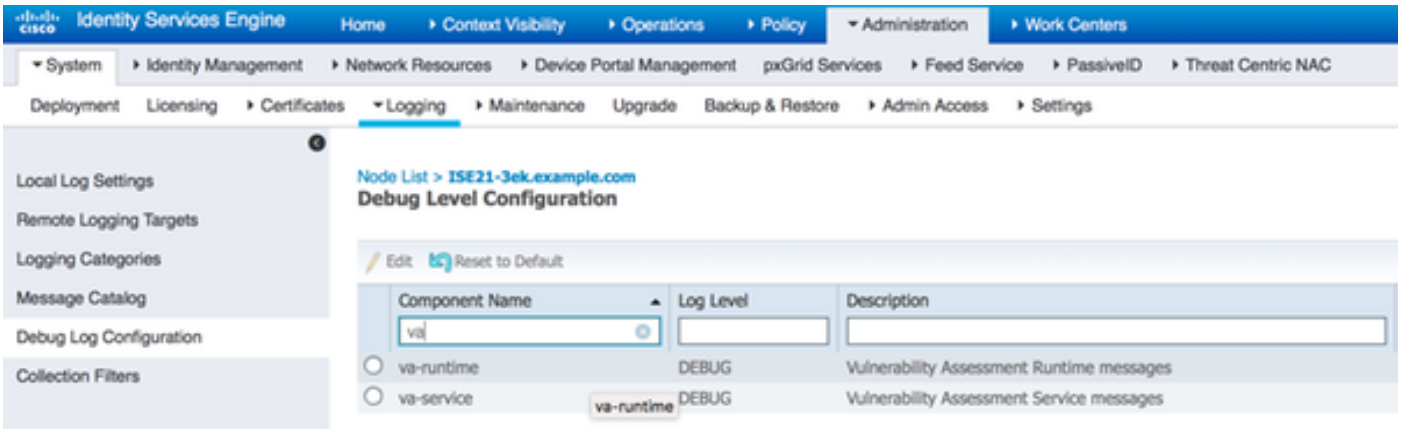

レポート自体では、[Detailed Results] に、検出された脆弱性が表示されます。




# トラブルシューティング

## ISE でのデバッグ

ISE 上でデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration] で TC-NAC ノードを選択し、[Log Level va-runtime] と [va-service] コンポーネントを [DEBUG] に変更します。




チェック対象のログは varuntime.log です。 ISE CLI から直接次の tail コマンドを発行します。

```
ISE21-3ek/admin# show logging application varuntime.log tail
```

TC-NAC Docker が、特定のエンドポイントに対するスキャン実行の指示を受け取ります。

```
2016-06-28 19:06:30,823 DEBUG  [Thread-70][] va.runtime.admin.mnt.EndpointFileReader -::::: --
VA: Read va runtime.
[{"[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicS
canEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
199fb81a4b99","psnHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}]
2016-06-28 19:06:30,824 DEBUG  [Thread-70][] va.runtime.admin.vaservice.VaServiceRemotingHandler
-::::: -- VA: received data from Mnt:
{"{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicSca
nEnabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
```

199fb81a4b99","psnHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}

結果を受信すると、すべての脆弱性データをコンテキスト ディレクトリに保存します。

2016-06-28 19:25:02,020 DEBUG  [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -::::: -- Got message from VaService:
[{"[{"macAddress":"C0:4A:00:14:8D:4B","ipAddress":"10.62.148.63","lastScanTime":1467134394000,"v
ulnerabilities":["{\"vulnerabilityId\":\"QID-90783\",\"cveIds\":\"CVE-2012-0002,CVE-2012-
0152,\",\"cvssBaseScore\":\"9.3\",\"cvssTemporalScore\":\"7.7\",\"vulnerabilityTitle\":\"Microso
ft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
38173\",\"cveIds\":\"\",\"cvssBaseScore\":\"9.4\",\"cvssTemporalScore\":\"6.9\",\"vulnerabilityT
itle\":\"SSL Certificate - Signature Verification Failed
Vulnerability\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90882\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.7\",\"cvssTemporalScore\":\"4\",\"vulnerabilityTit
le\":\"Windows Remote Desktop Protocol Weak Encryption Method
Allowed\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"vulnerabilityT
itle\":\"SMB Signing Disabled or SMB Signing Not
Required\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-
38601\",\"cveIds\":\"CVE-2013-2566,CVE-2015-
2808,\",\"cvssBaseScore\":\"4.3\",\"cvssTemporalScore\":\"3.7\",\"vulnerabilityTitle\":\"SSL/TLS
use of weak RC4 cipher\",\"vulnerabilityVendor\": \"\"Qualys\"}"]}]
2016-06-28 19:25:02,127 DEBUG  [pool-311-thread-8][]
va.runtime.admin.vaservice.VaServiceMessageListener -::::: -- VA: Save to context db,
lastscantime: 1467134394000, mac: C0:4A:00:14:8D:4B
2016-06-28 19:25:02,268 DEBUG  [pool-311-thread-8][]
va.runtime.admin.vaservice.VaAdminServiceContext -::::: -- VA: sending elastic search json to
pri-lan
2016-06-28 19:25:02,272 DEBUG  [pool-311-thread-8][]
va.runtime.admin.vaservice.VaPanRemotingHandler -::::: -- VA: Saved to elastic search:
{{C0:4A:00:14:8D:4B=[{"vulnerabilityId":"QID-90783","cveIds":"CVE-2012-0002,CVE-2012-
0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft Windows
Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)","vulnerabilityVendor":"Qualys"}, {"vulnerabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL
Certificate - Signature Verification Failed Vulnerability","vulnerabilityVendor": ""Qualys"},
{"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
Remote Desktop Protocol Weak Encryption Method Allowed","vulnerabilityVendor": ""Qualys"},
{"vulnerabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
Signing Disabled or SMB Signing Not Required","vulnerabilityVendor": ""Qualys"},
{"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-
2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLS use of weak
RC4 cipher","vulnerabilityVendor": ""Qualys"}]}

チェック対象の口グは vaservice.log です。 ISE CLI から直接次の tail コマンドを発行します。

```
ISE21-3ek/admin# show logging application vaservice.log tail
```

次の脆弱性アセスメント要求がアダプタに送信されます。

2016-06-28 17:07:13,200 DEBUG  [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil -
::::: -- VA SendSyslog systemMsg :
[{"[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA request submitted to
adapter","TC-NAC.Details","VA request submitted to adapter for processing","TC-

```
NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IpAddress","10.62.148.63","TC-
NAC.AdapterInstanceUuid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-
NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]
```

AdapterMessageListener が、スキャンが終了するまで 5 分ごとにスキャンの状態を確認します。

```
2016-06-28 17:09:43,459 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number of endpoints queued for
checking scan results: 1, Number of endpoints queued for scan: 0, Number of endpoints for which
the scan is in progress: 0"}
2016-06-28 17:14:43,760 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number of endpoints queued for
checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which
the scan is in progress: 1"}
2016-06-28 17:19:43,837 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number of endpoints queued for
checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which
the scan is in progress: 1"}
2016-06-28 17:24:43,867 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number of endpoints queued for
checking scan results: 0, Number of endpoints queued for scan: 0, Number of endpoints for which
the scan is in progress: 1"}
```

アダプタが QID、CVE、および CVSS スコアを取得します。

```
2016-06-28 17:24:57,556 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"requestedMacAddress":"C0:4A:00:14:8D:4B","scanStatus":"ASSESSMENT_SUCCESS","lastScanTimeLong
":1467134394000,"ipAddress":"10.62.148.63","vulnerabilities":[{"vulnerabilityId":"QID-
38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL
Certificate - Signature Verification Failed
Vulnerability","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
Signing Disabled or SMB Signing Not
Required","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-90783","cveIds":"CVE-2012-
0002,CVE-2012-
0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft Windows
Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-
2566,CVE-2015-
2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLS use of weak
RC4 cipher","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
Remote Desktop Protocol Weak Encryption Method Allowed","vulnerabilityVendor": ""Qualys"}]}
2016-06-28 17:25:01,282 INFO   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Endpoint Details sent to IRF is
{"C0:4A:00:14:8D:4B":[{"vulnerability":{"CVSS_Base_Score":9.4,"CVSS_Temporal_Score":7.7},"time-
stamp":1467134394000,"title":"Vulnerability","vendor":"Qualys"}]}
2016-06-28 17:25:01,853 DEBUG  [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
::::: -- VA SendSyslog systemMsg :
[{"[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA successfully
completed","TC-NAC.Details","VA completed; number of vulnerabilities found: 5","TC-
NAC.MACAddress","C0:4A:00:14:8D:4B","TC-NAC.IpAddress","10.62.148.63","TC-
NAC.AdapterInstanceUuid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-
```

NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]

## よくある問題

### 問題点 1：ISE が取得したレポートでは CVSS_Base_Score は 0.0、CVSS_Temporal_Score は 0.0 だが、Qualys クラウドのレポートには検出された脆弱性が表示されている。

**問題：**

Qualys クラウドからのレポートには検出された脆弱性が表示されているが、ISE には脆弱性が表示されない。

vaservice.log には次のデバッグが表示されている。

```
2016-06-02 08:30:10,323 INFO   [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Endpoint Details sent to IRF is
{"C0:4A:00:15:75:C8":[{"vulnerability":{"CVSS_Base_Score":0.0,"CVSS_Temporal_Score":0.0},"time-
stamp":1464855905000,"title":"Vulnerability","vendor":"Qualys"}]}
```

**解決策：**

CVSS スコアがゼロになるのは、脆弱性がないためか、または、Qualys クラウドでの CVSS スコアの有効化が UI を使用してアダプタを設定する前に行われなかったためです。 CVSS スコア機能の有効化が記載されたナレッジ ベースは、アダプタが初めて設定された後にダウンロードされます。 CVSS の有効化は、ISE にアダプタ インスタンスが作成される前に行う必要があります。 これは、[Vulnerability Management] > [Reports] > [Setup] > [CVSS] > [Enable CVSS Scoring] で実行できます。

### 問題点 2：正しい許可ポリシーが一致するにもかかわらず、結果が Qualys クラウドから ISE に返送されない。

**問題：**

修正された許可ポリシーが一致したため、VA スキャンがトリガーされるはずである。 にもかかわらず、スキャンが実行されない。

vaservice.log には次のデバッグが表示されている。

```
2016-06-28 16:19:15,401 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
((Body:'[B@6da5e620(byte[311])'MessageProperties [headers={}, timestamp=null, messageId=null,
userId=null, appId=null, clusterId=null, type=null, correlationId=null, replyTo=null,
contentType=application/octet-stream, contentEncoding=null, contentLength=0,
deliveryMode=PERSISTENT, expiration=null, priority=0, redelivered=false,
receivedExchange=irf.topic.va-reports, receivedRoutingKey=, deliveryTag=9830, messageCount=0])
2016-06-28 16:19:15,401 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Message from adapter :
{"{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"Erro
r triggering scan: Error while trigeringon-demand scan code and error as follows 1904: none of
the specified IPs are eligible for Vulnerability Management
scanning.","lastScanTimeLong":0,"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15,771 DEBUG  [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -::::: -- Adapter scan result failed for
Macaddress:24:77:03:3D:CF:20, IP Address(DB): 10.201.228.102, setting status to failed
2016-06-28 16:19:16,336 DEBUG  [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
::::: -- VA SendSyslog systemMsg :
[{"[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
```

NAC.ServiceName","Vulnerability Assessment Service","TC-NAC.Status","VA Failure","TC-NAC.Details","Error triggering scan: Error while trigering on-demand scan code and error as follows 1904: none of the specified IPs are eligible for Vulnerability Management scanning.","TC-NAC.MACAddress","24:77:03:3D:CF:20","TC-NAC.IpAddress","10.201.228.102","TC-NAC.AdapterInstanceUuid","796440b7-09b5-4f3b-b611-199fb81a4b99","TC-NAC.VendorName","Qualys","TC-NAC.AdapterInstanceName","QUALYS_VA"]}]

**解決策：**

Qualys クラウドは、エンドポイントの IP アドレスがスキャンの対象ではないことを示しています。[Vulnerability Management] > [Assets] > [Host Assets] > [New] > [IP Tracked Hosts] で、IP アドレスがエンドポイントに追加されていることを確認してください。

# 参考資料

- Cisco Identity Services Engine 管理者ガイド リリース 2.1
- テクニカル サポートとドキュメント – Cisco Systems
- ビデオ： ISE 2.1 with Qualys
- Qualys に関するドキュメント