Configurez ISE 2.1 NAC Menace-central (TC-NAC) avec Qualys

Contenu

Introduction

Ce document décrit comment configurer le NAC Menace-central avec Qualys sur le Cisco Identity Services Engine (ISE) 2.1. La caractéristique centrale du contrôle d'accès au réseau de menace (TC-NAC) te permet de créer des stratégies d'autorisation basées sur les attributs de menace et de vulnérabilité reçus des adaptateurs de menace et de vulnérabilité.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Engine de gestion d'identité de Cisco
- Qualys ScanGuard

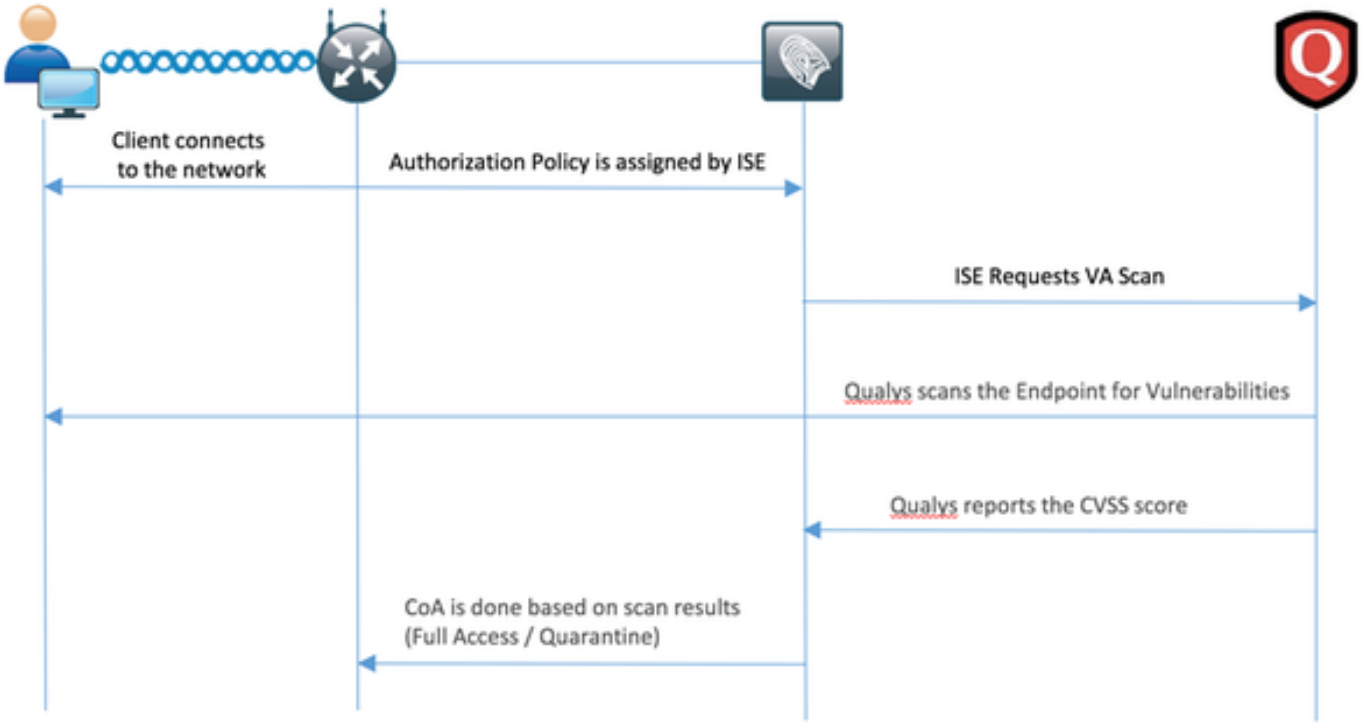
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.1 d'engine de gestion d'identité de Cisco
- Contrôleur LAN Sans fil (WLC) 8.0.121.0
- Scanner 8.3.36-1 de protection de Qualys, signatures 2.3.364-2
- Service Pack 1 de Windows 7

Configurer

Organigramme de haut niveau



C'est l'écoulement :

1. Le client se connecte au réseau, l'accès limité est donné et le profil avec **évaluent des vulnérabilités que la** case à cocher activée est assignée
2. Le noeud RPC envoie le message de Syslog au noeud MNT confirmant l'authentification a eu lieu et le balayage VA était le résultat de la stratégie d'autorisation
3. Le noeud MNT soumet le BALAYAGE au noeud TC-NAC (utilisant admin WebApp) utilisant ces données :
   - Adresse MAC
   - Adresse IP
   - Scan interval
   - Balayage périodique activé
   - Lancer le RPC
4. Qualys TC-NAC (encapsulé dans le conteneur de docker) communique avec le nuage de

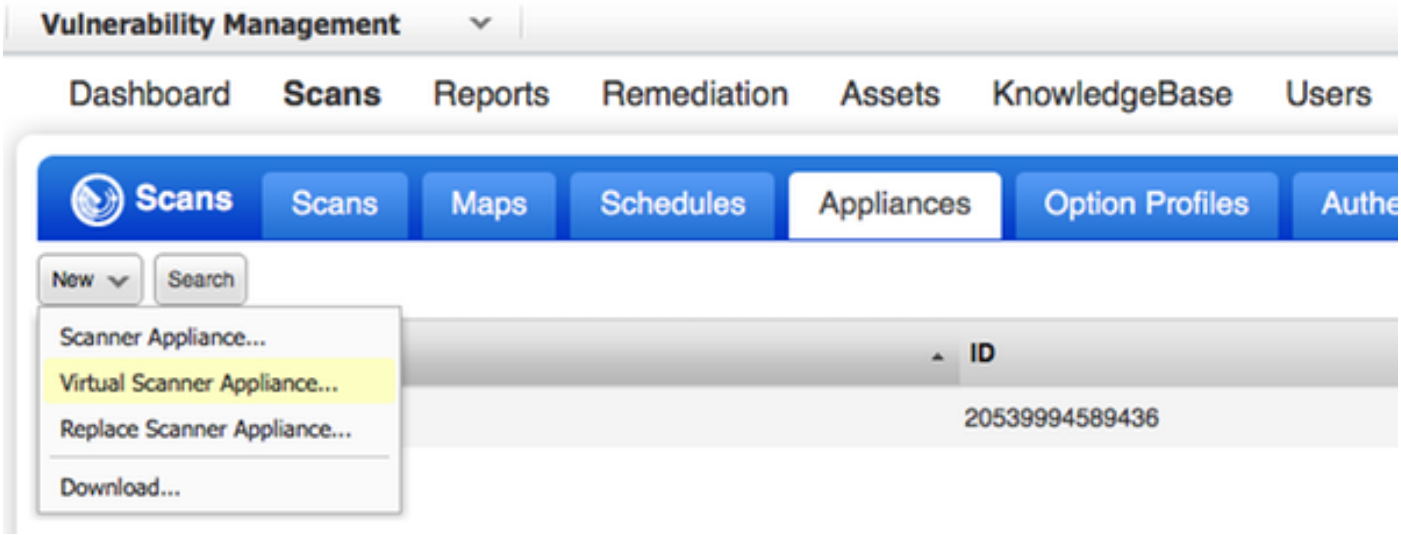
Qualys (par l'intermédiaire de REPOS API) pour déclencher le balayage si nécessaire
5. Le nuage de Qualys demande au scanner de Qualys pour balayer le point final
6. Le scanner de Qualys envoie les résultats du balayage au nuage de Qualys
7. Des résultats du balayage sont renvoyés à TC-NAC :
   - Adresse MAC
   - Tous les scores CVSS
   - Toutes les vulnérabilités (QID, titre, CVEIDs)
8. TC-NAC met à jour la CASSEROLE avec toutes les données de l'étape 7.
9. Le CoA est déclenché si nécessaire selon la stratégie configurée d'autorisation.

Configurez le nuage et le scanner de Qualys

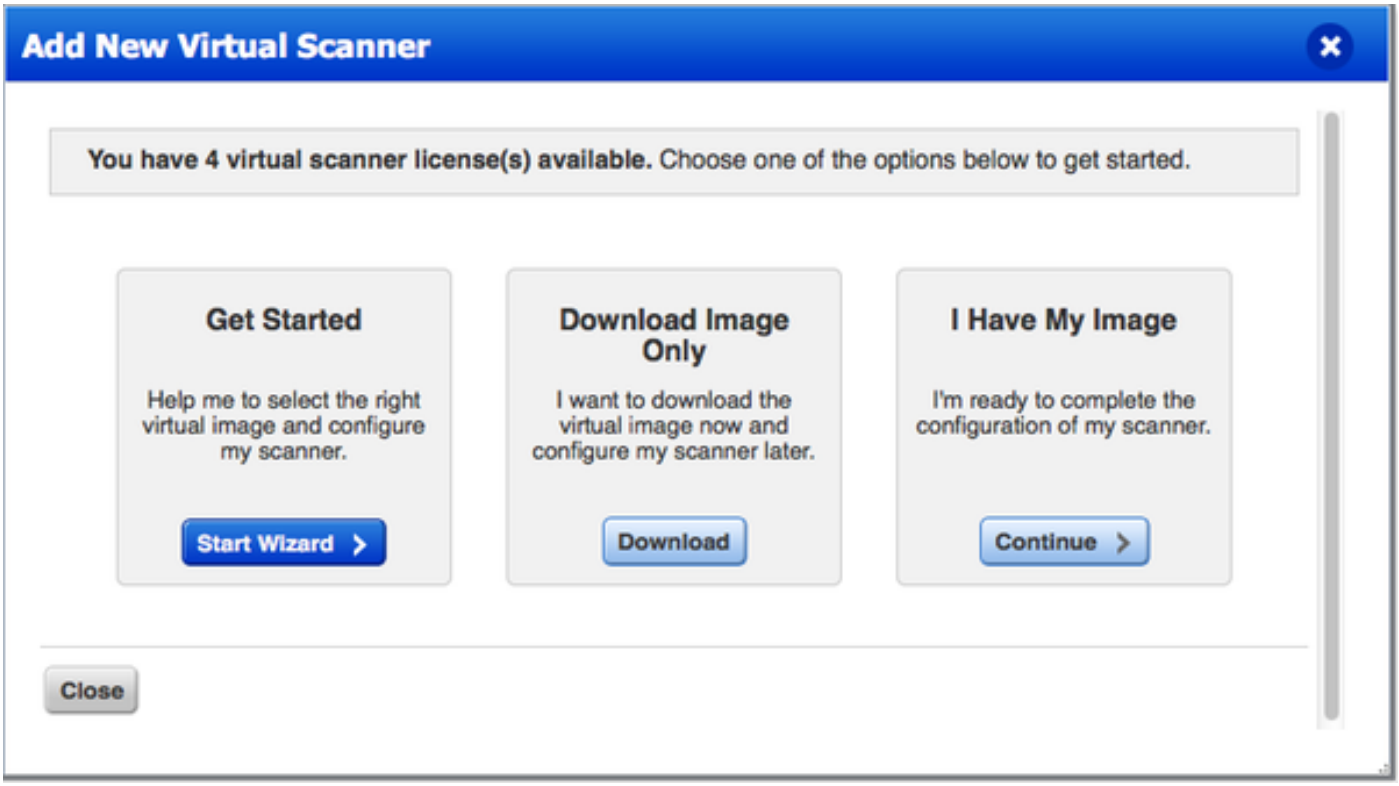
> **Attention** : La configuration de Qualys dans ce document est faite pour le laboratoire, consultent s'il vous plaît des ingénieurs de Qualys pour des considérations de conception

Étape 1. Déployez le scanner de Qualys

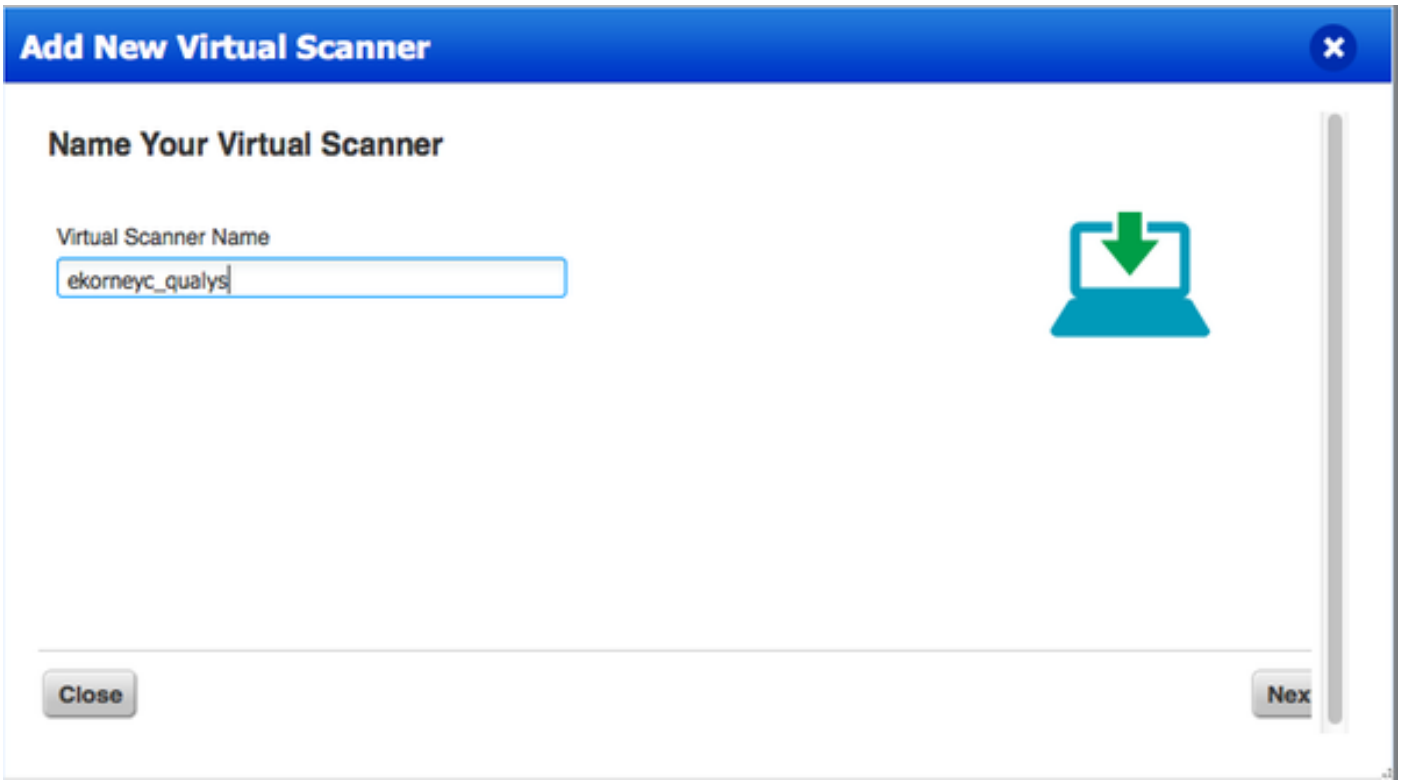
Le scanner de Qualys peut être déployé à partir du fichier d'OVULES. Ouvrez une session au nuage de Qualys et naviguez vers des balayages > des appliances et sélectionnez la nouvelle > virtuelle appliance de scanner



Sélectionnez l'**image de téléchargement seulement** et sélectionnez la distribution appropriée



Pour obtenir le code de lancement que vous pouvez aller aux balayages > aux appliances et nouvelle > virtuelle appliance choisie de scanner et me sélectionner **ai mon image**



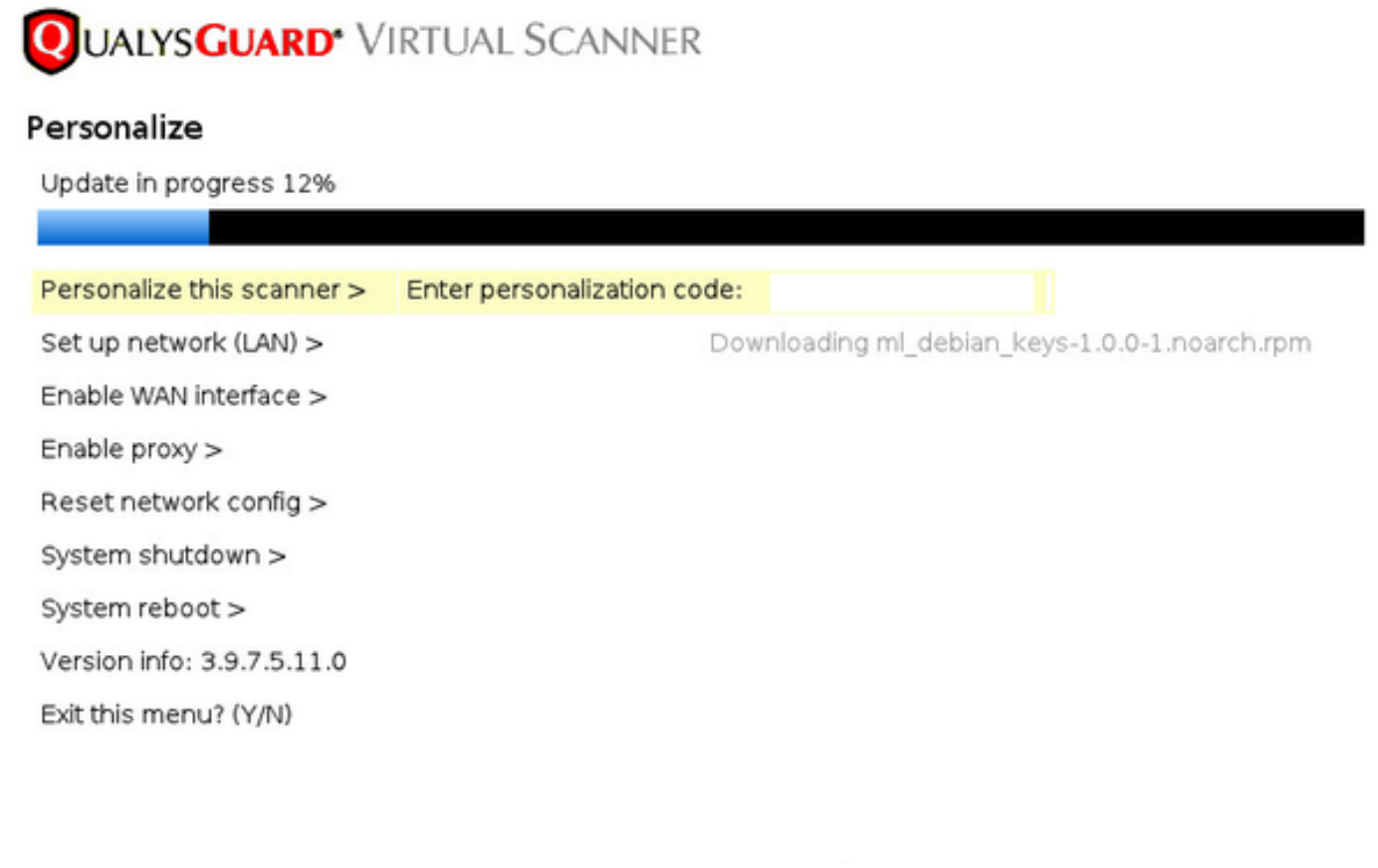
Après avoir écrit le nom de scanner vous êtes donné le code d'autorisation que vous utiliserez plus tard.

Étape 2. Configurez le scanner de Qualys

Déployez les OVULES sur la plate-forme de virtualisation de votre choix. Une fois que fait, configurez ces configurations :

- Réseau d'installation (RÉSEAU LOCAL)
- Configurations d'interface WAN (si vous utilisez deux interfaces)
- Paramètres de proxy (si vous utilisez le proxy)
- Personnalisez ce scanner

Après le scanner se connecte à Qualys et télécharge le derniers logiciel et signatures.



Pour vérifier le scanner t'est connecté peut naviguer vers des balayages > des appliances.

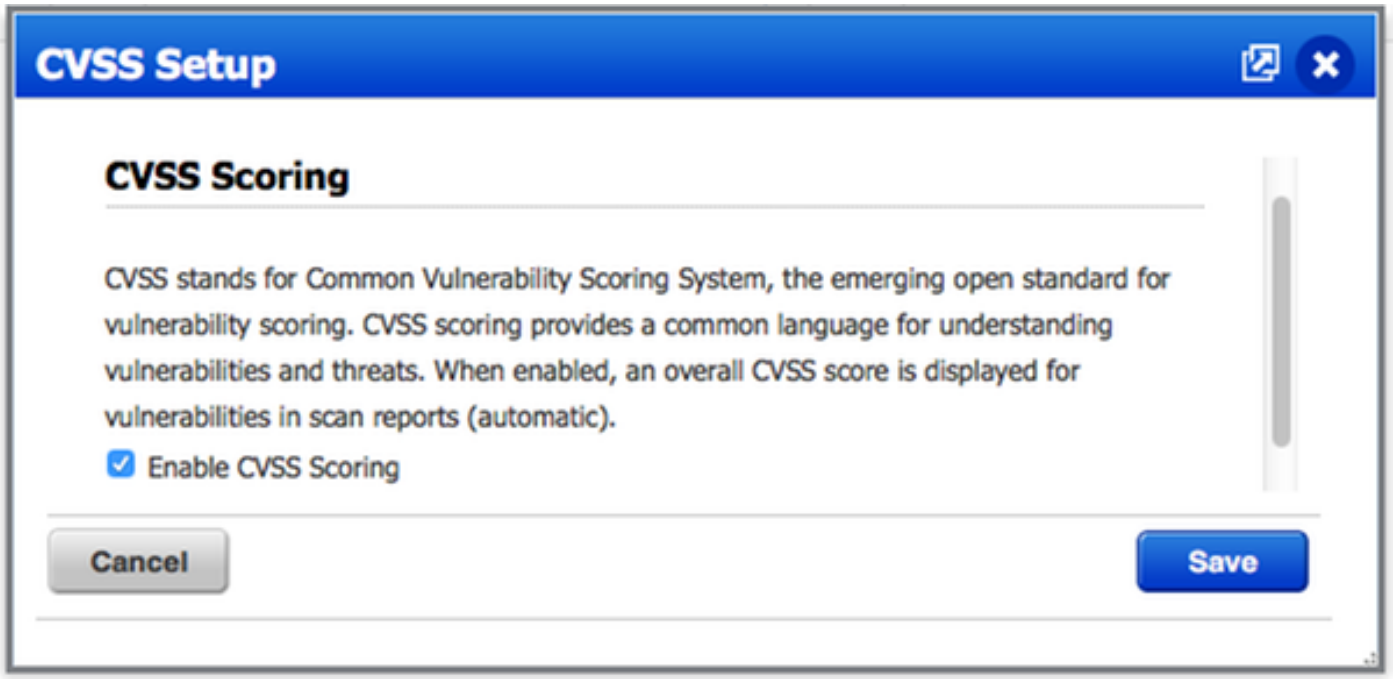
Le vert connecté se connectent la gauche indique que le scanner est prêt, vous peut également voir l'IP de RÉSEAU LOCAL, l'IP de WAN, la version du scanner et les signatures.

Configurez ISE

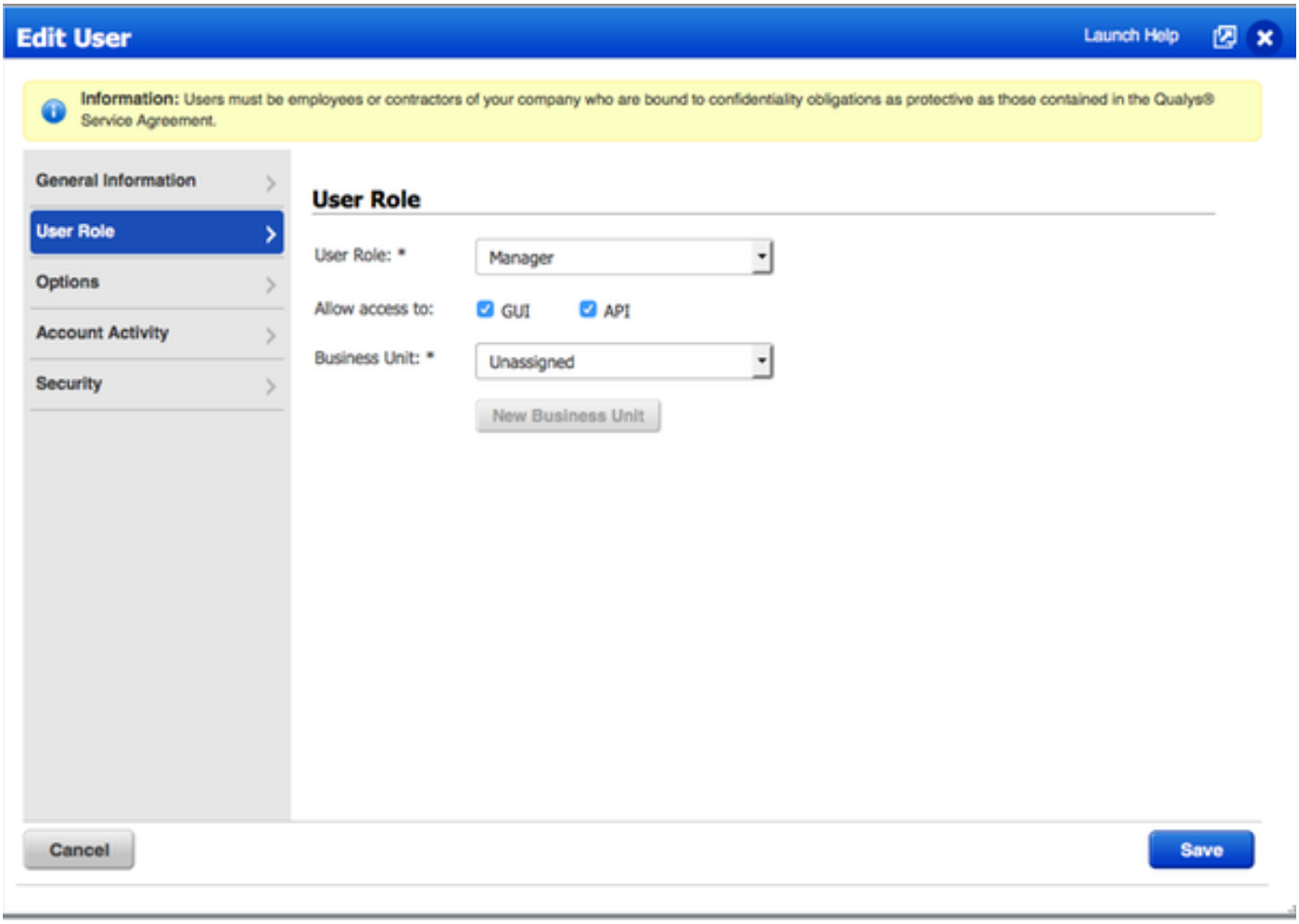
Bien que vous ayez configuré le scanner et le nuage de Qualys, vous devez encore accorder des configurations de nuage pour s'assurer que l'intégration avec ISE fonctionne bien. Note, il devrait être fait avant que vous configuriez l'adaptateur par le GUI, car la base de connaissances contenant le marquage CVSS est téléchargée après que l'adaptateur soit configuré pour la première fois.

Étape 1. Configurations de nuage de Qualys d'optimisation pour l'intégration avec ISE

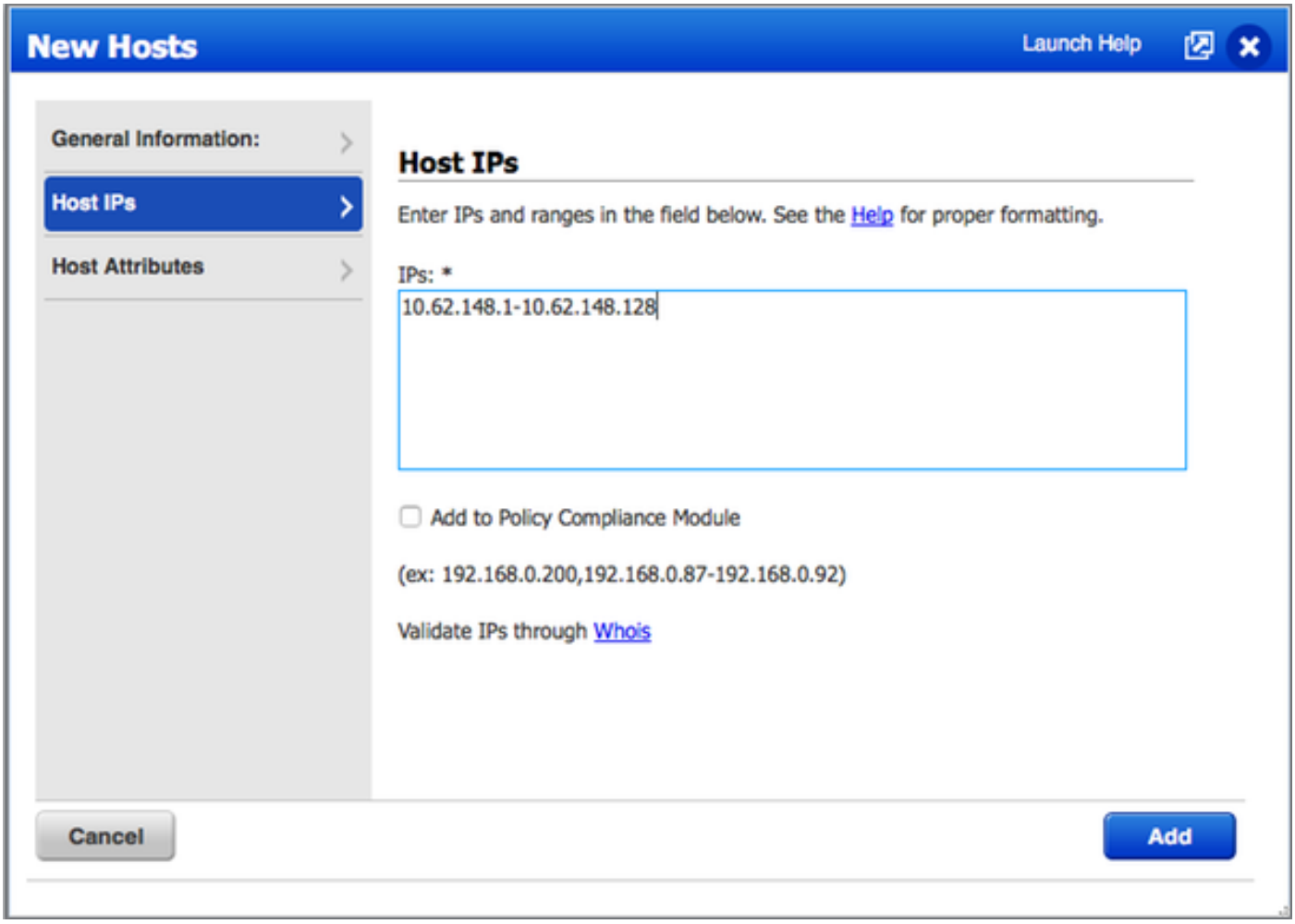
- L'enable CVSS marquant à la Gestion de vulnérabilité > signale > installé > CVSS > marquage de l'enable CVSS



- Assurez-vous que les identifiants utilisateurs utilisés dans la configuration d'adaptateur ont des privilèges de gestionnaire. Sélectionnez votre utilisateur du coin supérieur gauche et cliquez sur en fonction le **profil utilisateur**. Vous devriez avoir des droits de gestionnaire dans le **rôle de l'utilisateur.**



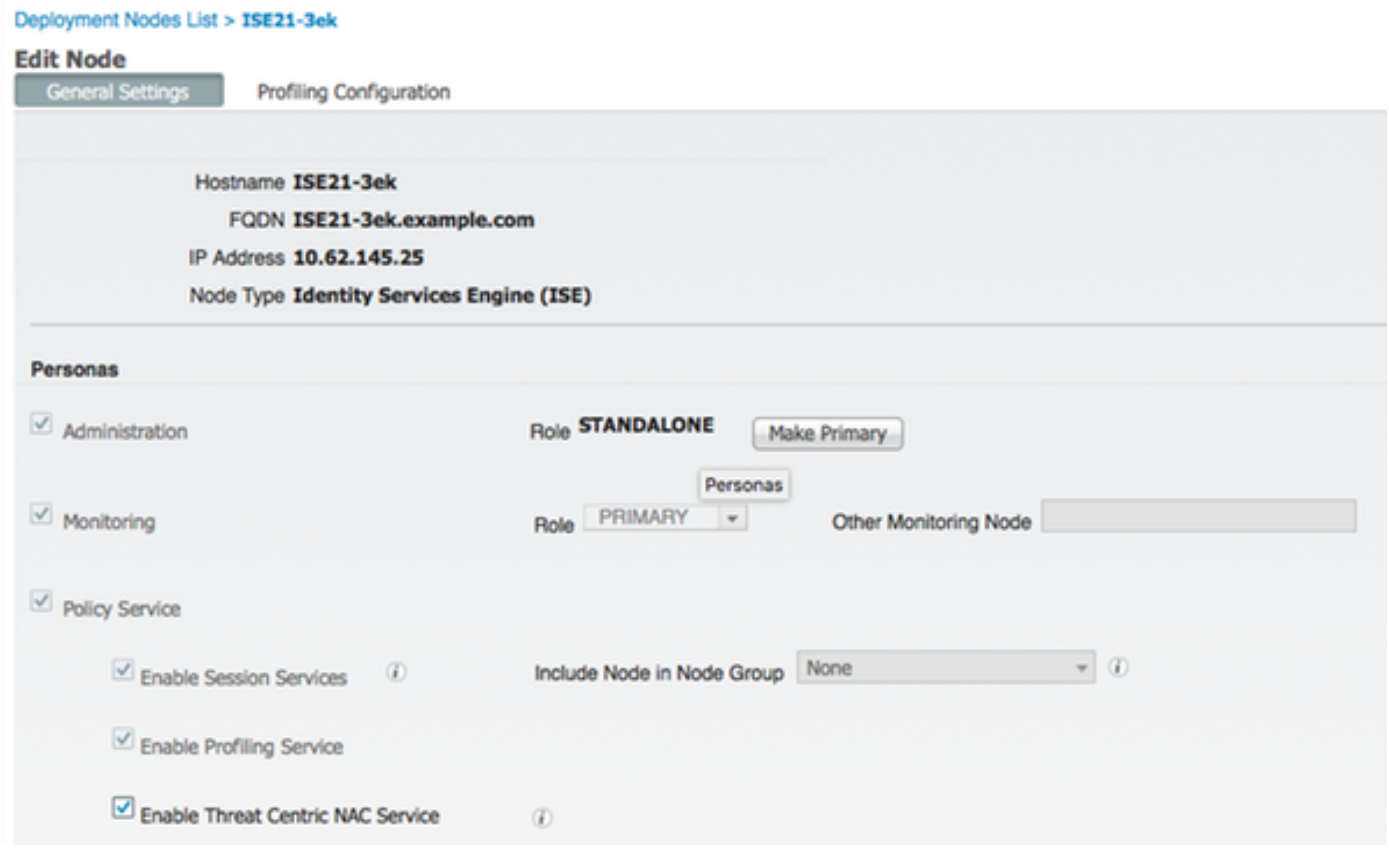
- Assurez-vous que des adresses IP/sous-réseaux des points finaux qui exigent l'estimation de vulnérabilité sont ajoutés à Qualys à la Gestion de vulnérabilité > aux ressources > aux ressources en hôte > nouveau > les hôtes dépistés par IP



Étape 2. Services de l'enable TC-NAC

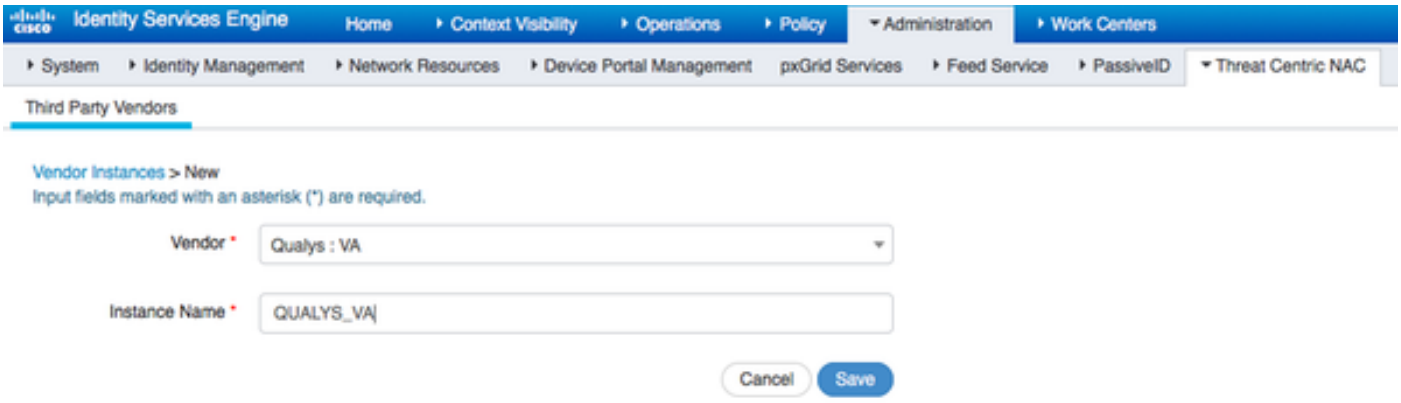
Les services de l'enable TC-NAC sous la gestion > le déploiement > éditent le noeud. Case à cocher **centrale de service de la menace NAC d'enable** de contrôle.

> **Note**: Il peut y avoir seulement un noeud TC-NAC par déploiement.

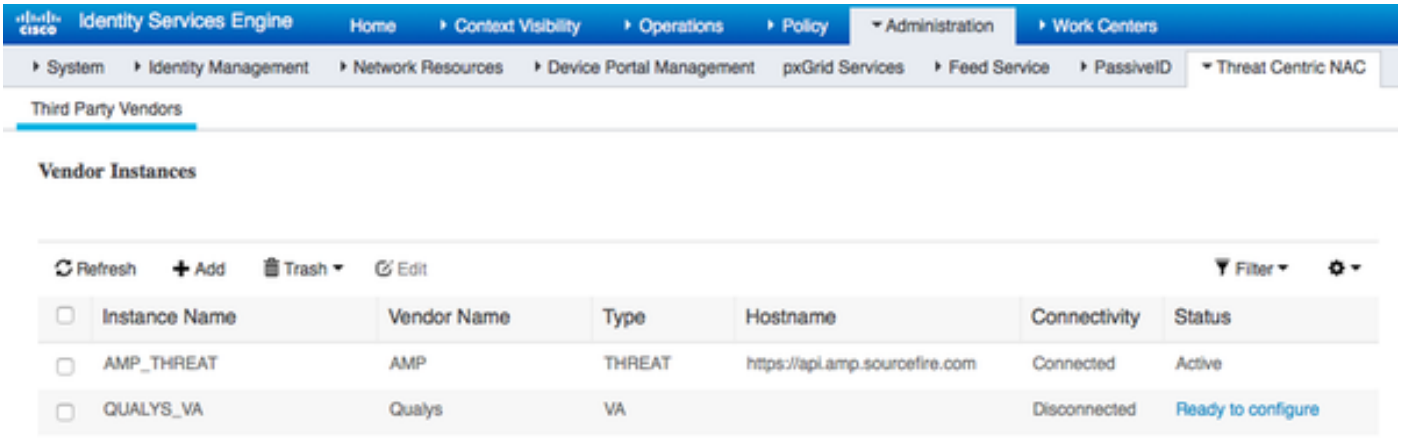


Étape 3. Configurez la Connectivité d'adaptateur de Qualys au cadre ISE VA

Naviguez vers la gestion > la menace centrales NAC > constructeurs tiers > ajoutent. Cliquez sur en fonction la **sauvegarde**.

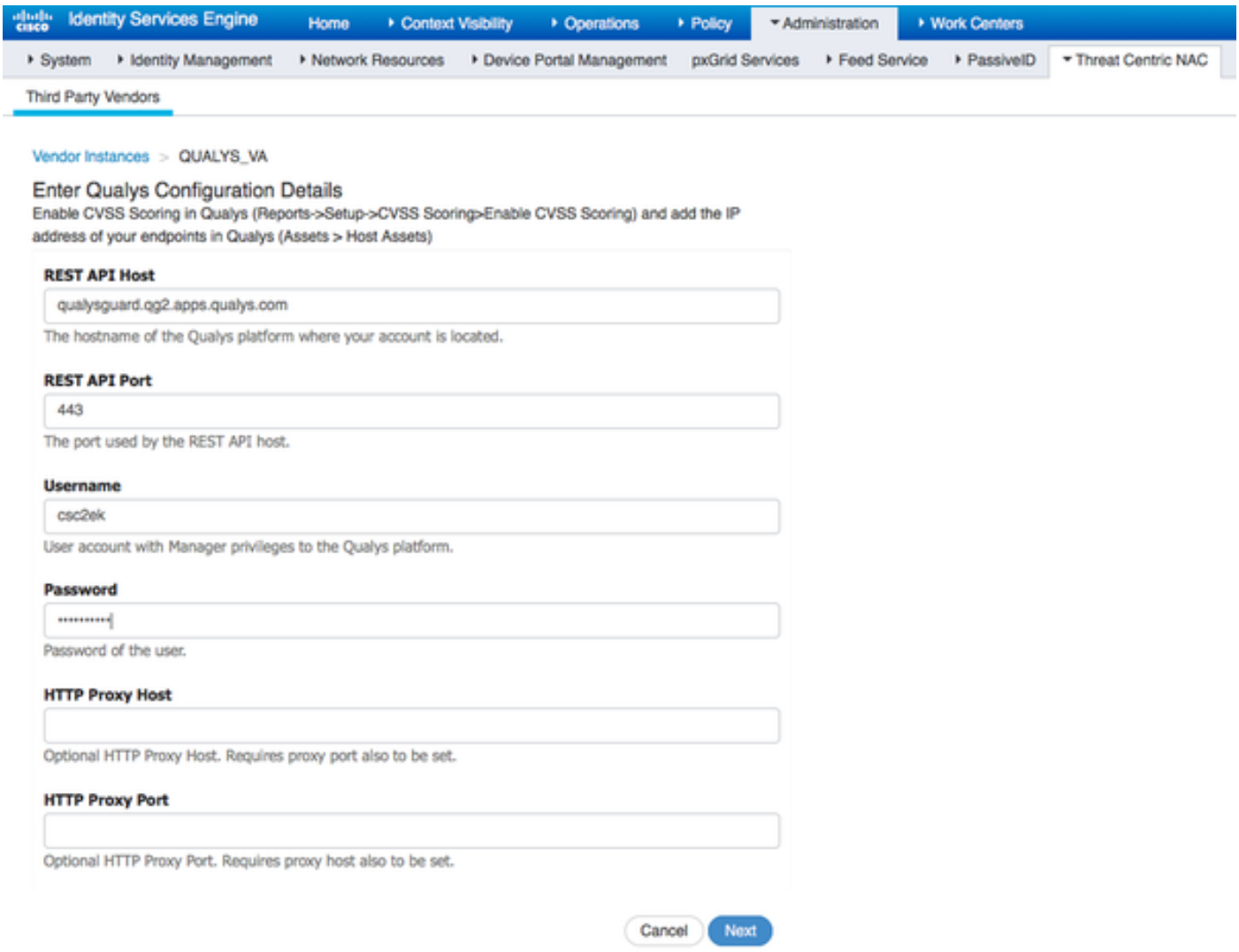


Quand les transitions d'exemple de Qualys **à préparer pour configurer l'**état, cliquent sur en fonction **prêt à configurer l'**option dans l'état.

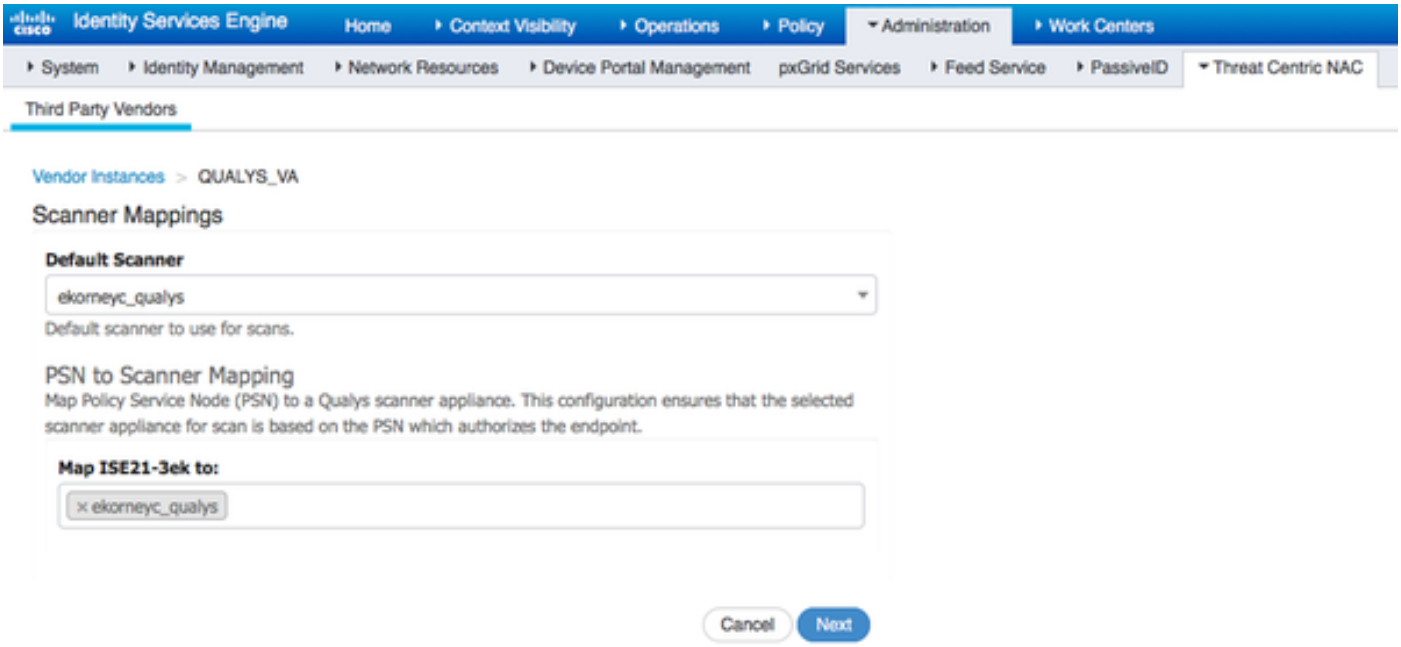


L'hôte du REPOS API devrait être celui que vous utilisez pour le nuage de Qualys, où votre compte se trouve. Dans cet exemple - qualysguard.qg2.apps.qualys.com

Le compte devrait être celui avec des privilèges de gestionnaire, cliquent sur en fonction **ensuite**.

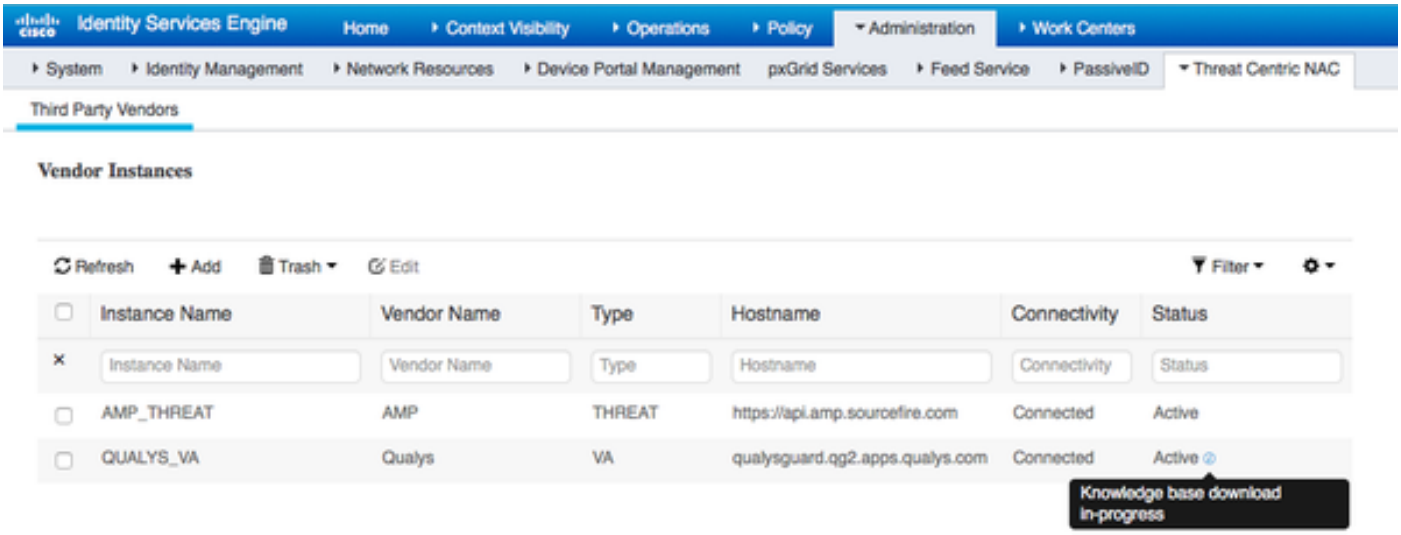


ISE télécharge des informations sur les scanners qui sont connectés au nuage de Qualys, vous peut configurer le RPC au mappage de scanner à cette page. Il s'assure que le scanner sélectionné est sélectionné a basé sur le RPC qui autorise le point final.



Les paramètres avancés sont bien documentés du guide d'admin ISE 2.1, lien peuvent être trouvés dans la section de références de ce document. Cliquez sur en fonction **ensuite** et **terminez**. Transitions d'exemple de Qualys aux débuts de téléchargement d'**état active** et de base de connaissances.

Note: Il peut y avoir seulement un exemple de Qualys par déploiement.



Étape 4. Configurez le profil d'autorisation pour déclencher le balayage VA

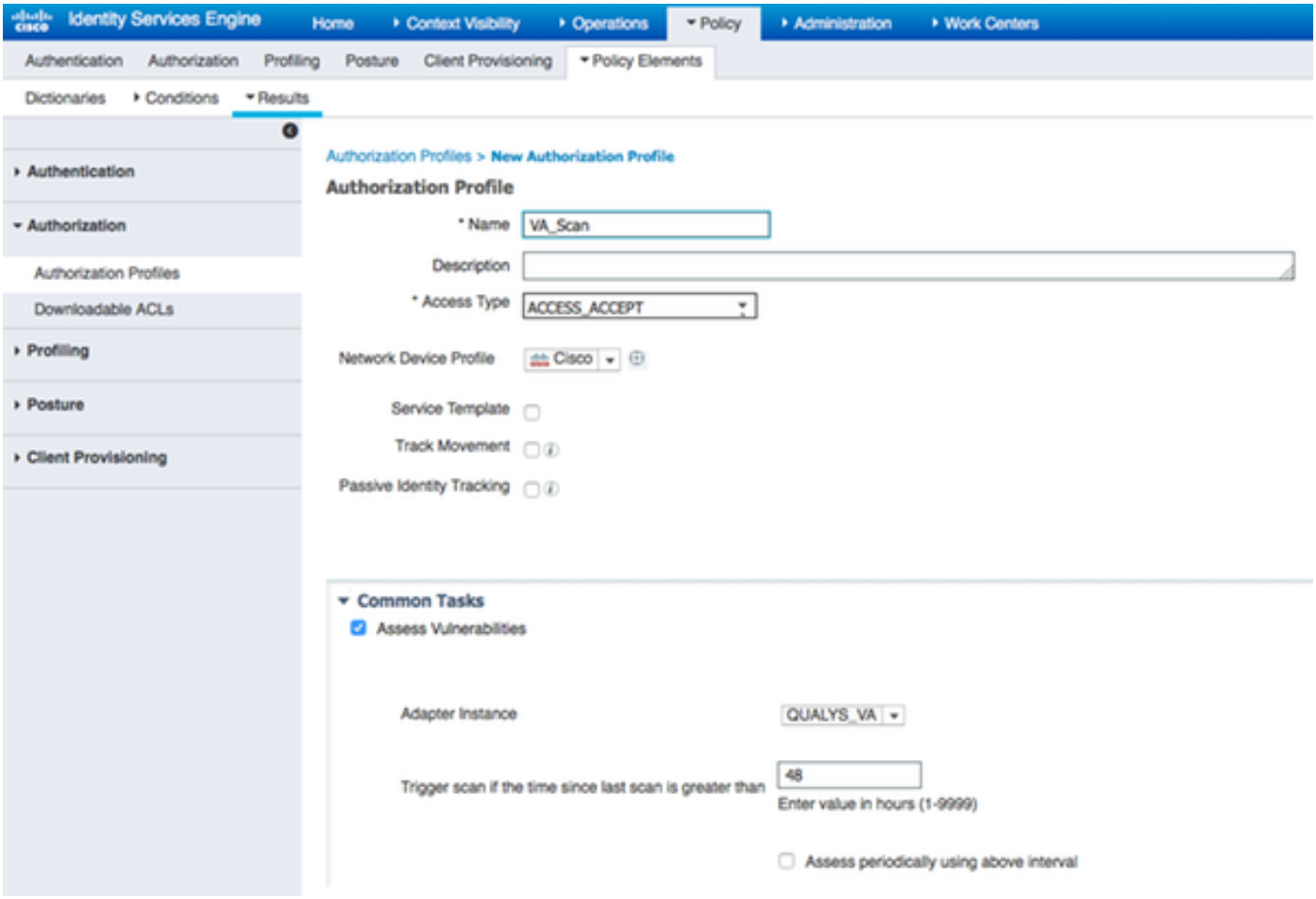
Naviguez vers la stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation. Ajoutez le nouveau profil. Sous des **fonctionnalités usuelles** sélectionnez la case à cocher d'**estimation de vulnérabilité**.
Le scan interval sur demande devrait être sélectionné selon votre conception de réseaux.

Le profil d'autorisation contient ces poids du commerce-paires :

Cisco-poids du commerce-paires = on-demand-scan-interval=48
Cisco-poids du commerce-paires = periodic-scan-enabled=0

Cisco-poids du commerce-paires = va-adapter-instance=796440b7-09b5-4f3b-b611-199fb81a4b99

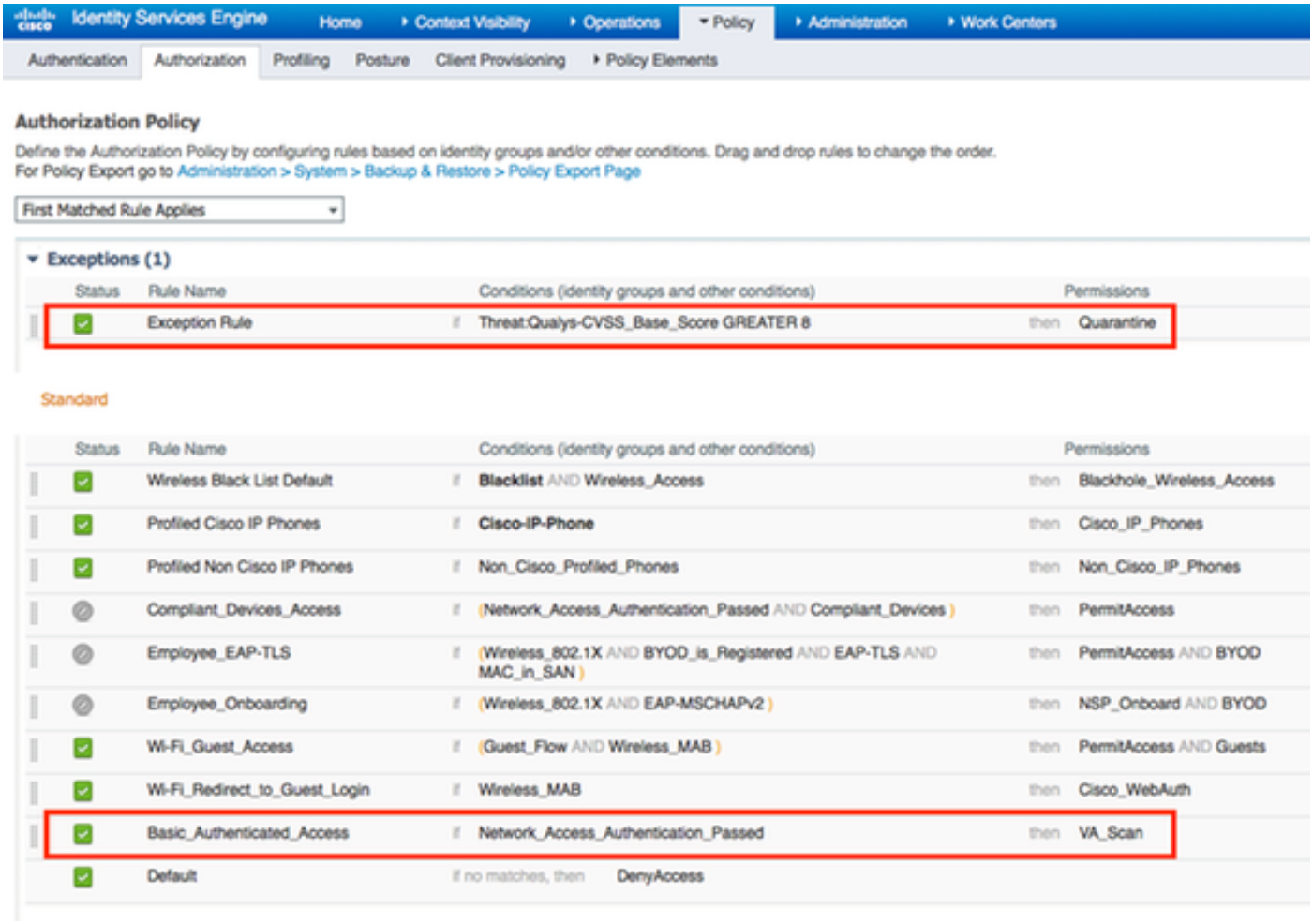
Ils sont envoyés aux périphériques de réseau dans le paquet d'acceptation d'accès, bien que l'objectif réel de eux soit de dire le noeud MNT que le balayage devrait être déclenché. Le MNT demande au noeud TC-NAC pour communiquer avec le nuage de Qualys.



Étape 5. Configurez les stratégies d'autorisation

- Configurez la stratégie d'autorisation pour utiliser le nouveau profil d'autorisation configuré dans l'étape 4. naviguent vers la stratégie > l'autorisation > la stratégie d'autorisation, localisent la règle de **Basic_Authenticated_Access** et cliquent sur en fonction **Edit**. Changez les autorisations de **PermitAccess au VA_Scan standard** de création récente. Ceci entraîne un balayage de vulnérabilité pour tous les utilisateurs. Cliquez sur en fonction la **sauvegarde**.

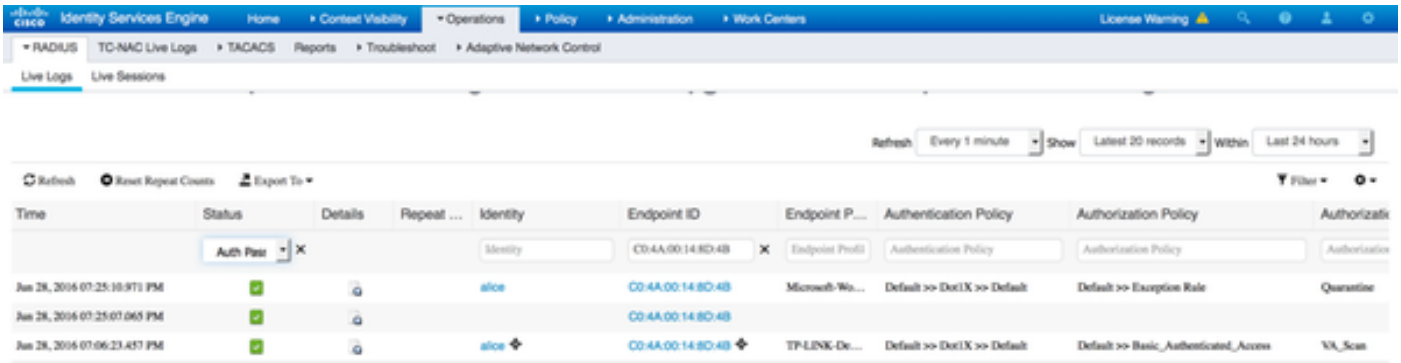
- Créez la stratégie d'autorisation pour des ordinateurs Quarantined. Naviguez vers la stratégie > l'autorisation > la stratégie > les exceptions d'autorisation et créez une **règle d'exception**. Cliquez sur en fonction les conditions > créent le nouvel état (option avancée) > attribut choisi, font descendre l'écran et sélectionnent la **menace**. Développez l'attribut de **menace** et sélectionnez **Qualys-CVSS_Base_Score**. Changez l'opérateur à **plus grand qu'**et écrivez une valeur selon votre stratégie de sécurité. Le profil d'autorisation de **quarantaine** devrait donner l'accès limité à l'ordinateur vulnérable.



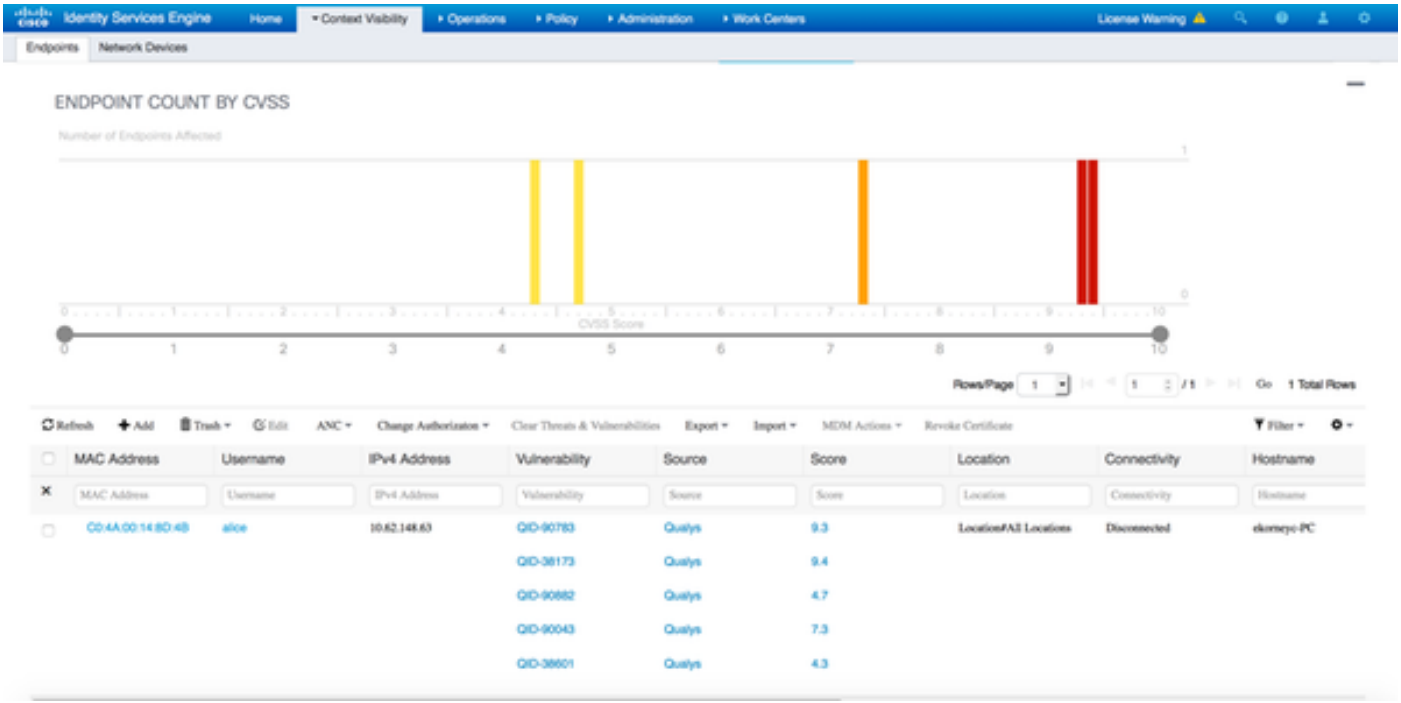
Vérifiez

Plateforme de services d'identité

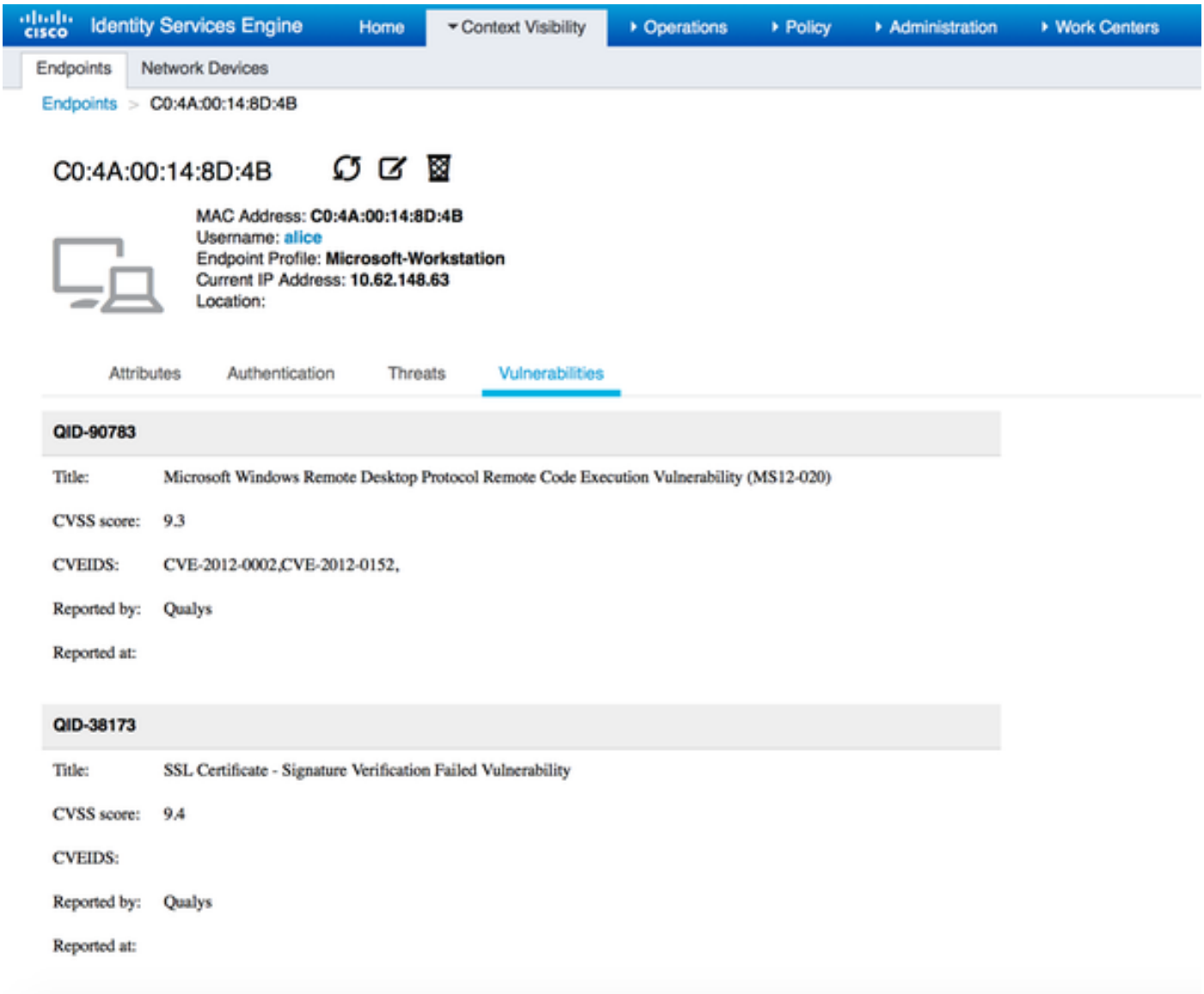
Le premier balayage VA de déclencheurs de connexion. Quand le balayage est de finition, la réauthentification CoA est déclenchée pour appliquer la nouvelle stratégie si elle est appariée.



Afin de vérifier quelles vulnérabilités ont été détectées, naviguez vers la visibilité de contexte > les points finaux. Vérifiez par vulnérabilités de points finaux avec les scores donnés à lui par Qualys.

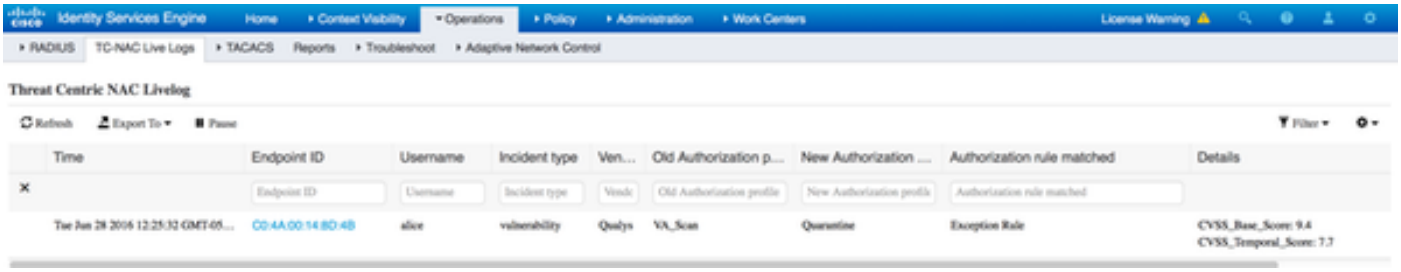


En sélectionnant le point final particulier, plus de détails au sujet de chaque vulnérabilité apparaît, y compris le **titre** et les **CVEID**.



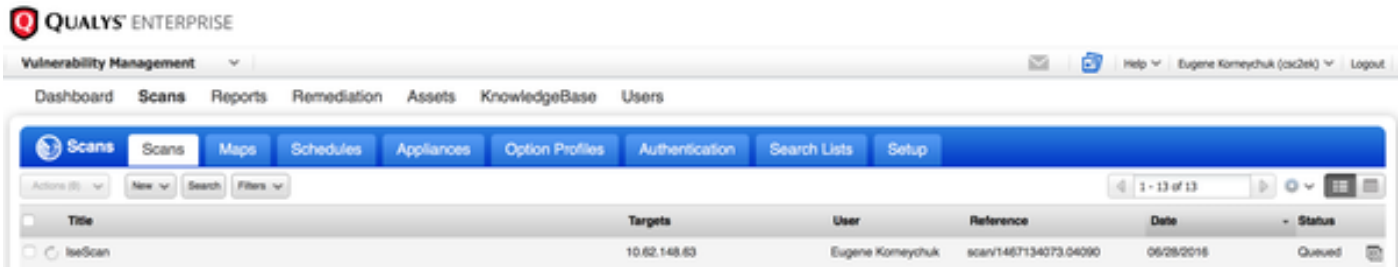
En fonctionnement > TC-NAC vivent les logs, vous pouvez voir vieux contre de nouvelles stratégies d'autorisation appliquées et détails sur CVSS_Base_Score.

> **Note**: Des états d'autorisation sont faits ont basé sur CVSS_Base_Score, qui égale au score de vulnérabilité le plus élevé détecté sur le point final.

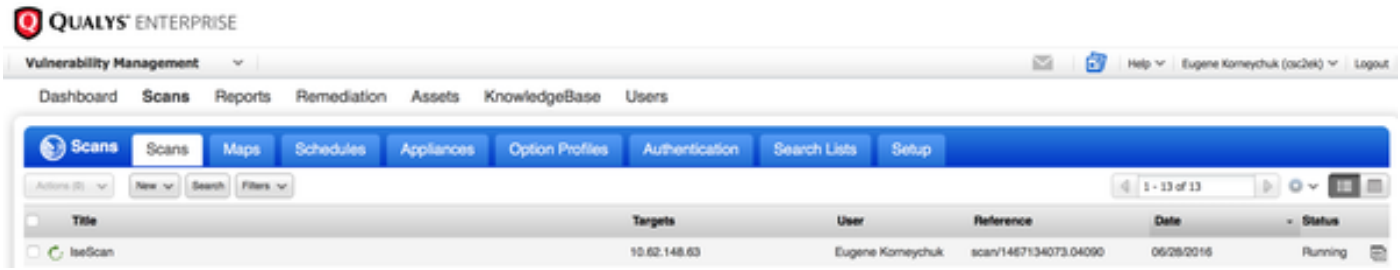


Nuage de Qualys

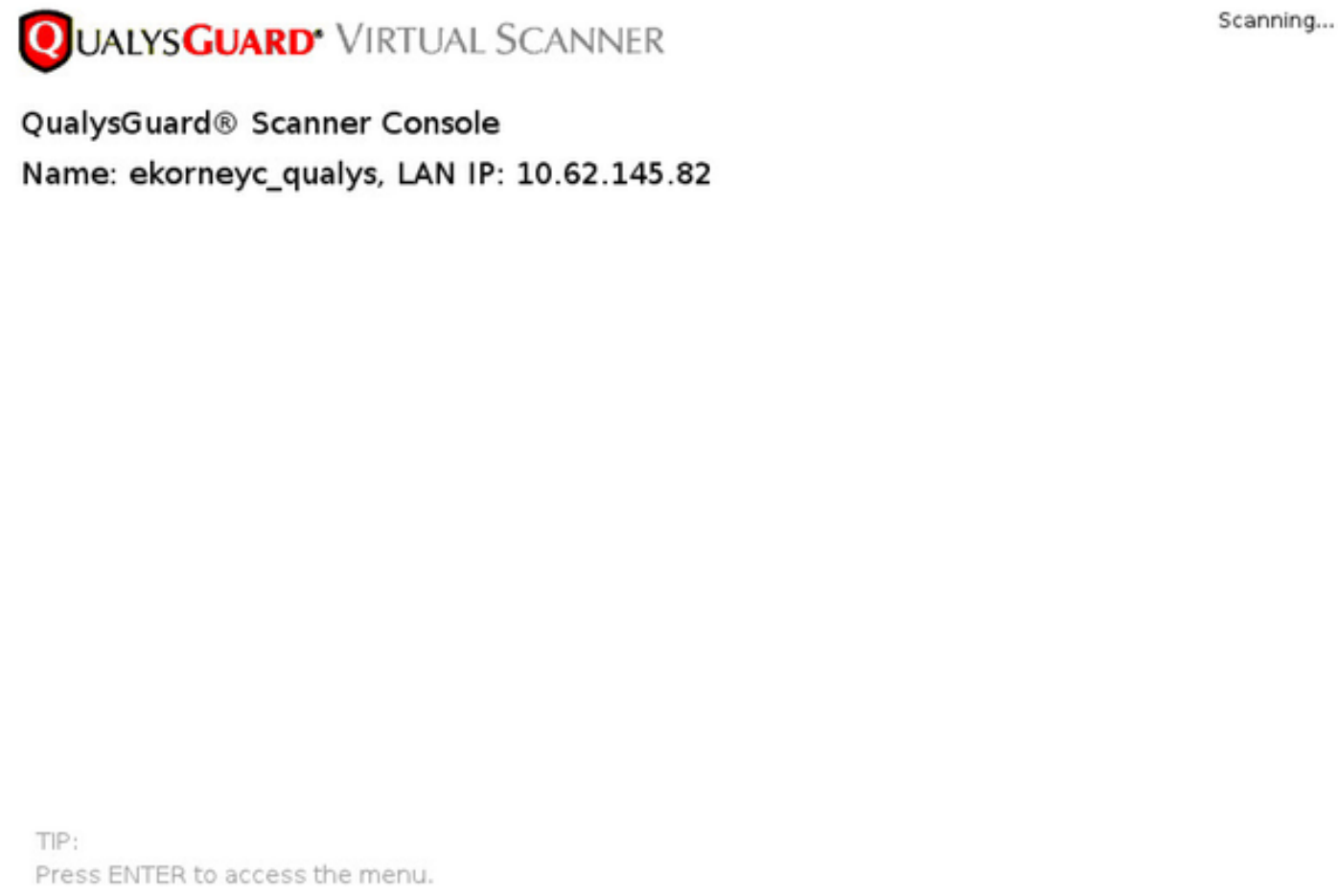
Quand le balayage VA est déclenché par TC-NAC Qualys aligne le balayage, il peut être visualisé aux balayages > aux balayages



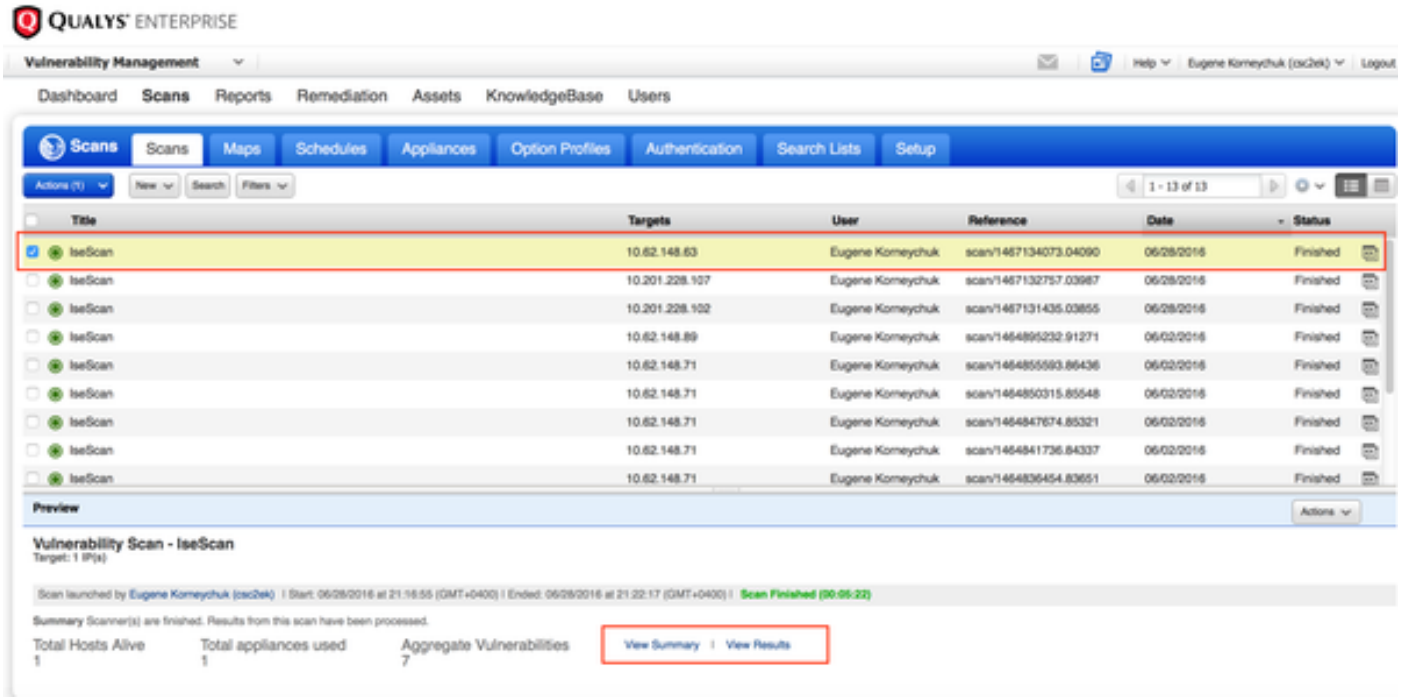
Après il des transitions à s'exécuter, signifiant le nuage de Qualys a demandé au scanner de Qualys d'exécuter la lecture réelle



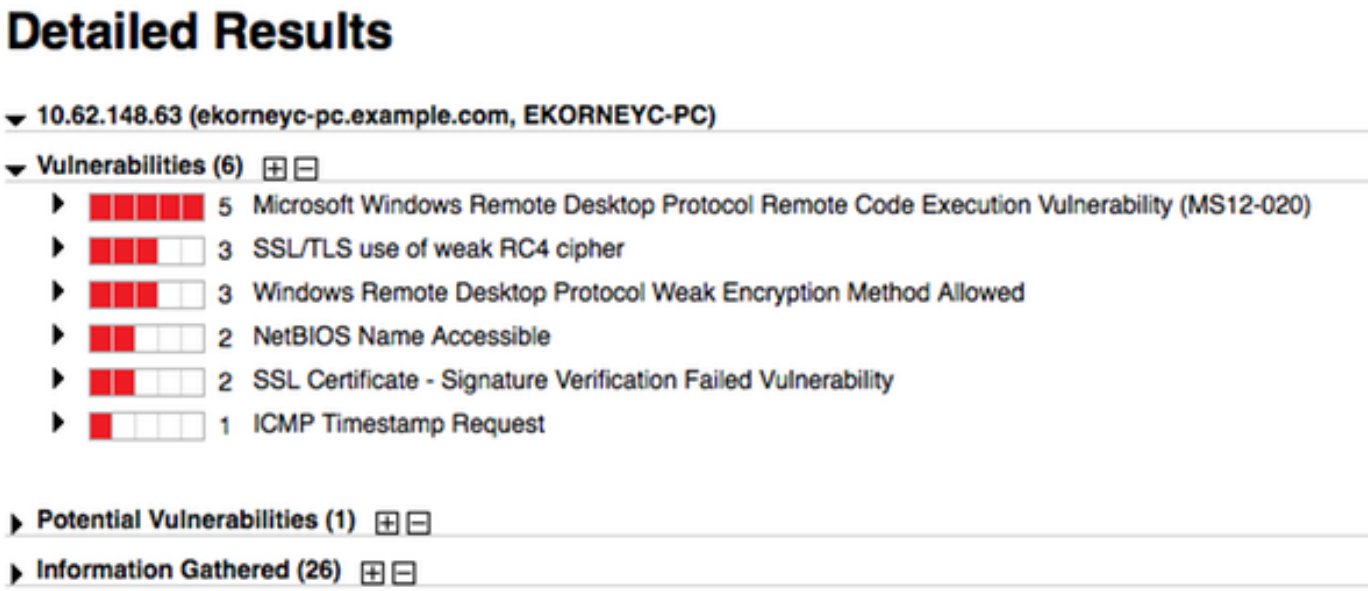
Tandis que le scanner exécute le balayage, vous devriez voir la « lecture… » signe dans l'angle supérieur droit de la protection de Qualys



Une fois le balayage l'est fait des transitions à l'état de finition. Vous pouvez visualiser des résultats aux balayages > aux balayages, balayage prié choisi et cliquer sur en fonction le **résumé de vue** ou les **résultats de vue**.



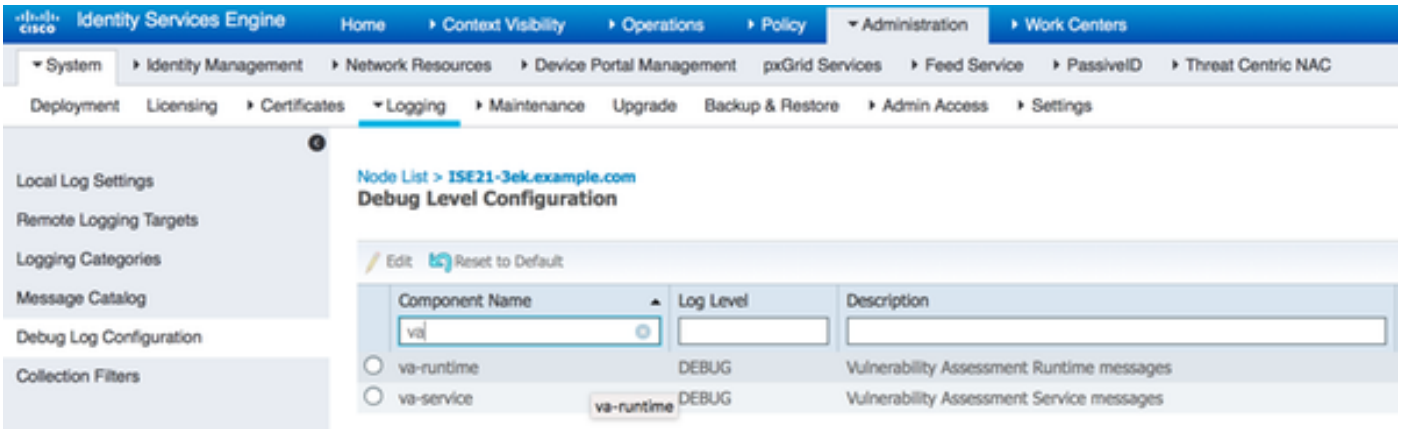
Dans l'état lui-même vous pouvez voir des **résultats détaillés**, où des vulnérabilités détectées sont affichées.



Dépanner

Debugs sur ISE

Afin d'activer met au point sur ISE naviguent vers la gestion > le système > se connectant > configuration de log de debug, noeud choisi TC-NAC et changent le composant de va-**délai d'exécution** et de va-**service de niveau de log POUR DÉBUGGER**



Logs à vérifier - varuntime.log. Vous pouvez le suivre directement d'ISE CLI :

```
Queue de varuntime.log d'application de show logging ISE21-3ek/admin#
```

Le docker TC-NAC a reçu l'instruction d'exécuter le balayage pour le point final particulier.

```
2016-06-28 DEBUG [Thread-70][] va.runtime.admin.mnt.EndpointFileReader de 19:06:30,823 - : : : :
: - VA : Lisez le délai d'exécution va.
[{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScan
Enabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
199fb81a4b99","psnHostName":"ISE21-3ek","heartBeatTime":0,"lastScanTime":0}]
2016-06-28 DEBUG [Thread-70][] va.runtime.admin.vaservice.VaServiceRemotingHandler de
19:06:30,824 - : : : : : - VA : données reçues de MNT :
{"operationType":1,"macAddress":"C0:4A:00:14:8D:4B","ondemandScanInterval":"48","isPeriodicScanE
nabled":false,"periodicScanEnabledString":"0","vendorInstance":"796440b7-09b5-4f3b-b611-
```

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

Une fois que le résultat est reçu il enregistre toutes les données de vulnérabilité dans le répertoire de contexte.

2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaServiceMessageListener de 19:25:02,020 - : : : : : - message reçu de VaService : Vulnérabilité d'exécution de code distant de Windows Remote Desktop Protocol de [{"macAddress":"C0:4A:00:14:8D:4B","ipAddress":"10.62.148.63","lastScanTime":1467134394000,"vulnerabilities":["{\"vulnerabilityId\":\"QID-90783\",\"cveIds\":\"CVE-2012-0002,CVE-2012-0152,\",\"cvssBaseScore\":\"9.3\",\"cvssTemporalScore\":\"7.7\",\"vulnerabilityTitle\":\"Microsoft (certificat de MS12-020)\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-38173\",\"cveIds\":\"\",\"cvssBaseScore\":\"9.4\",\"cvssTemporalScore\":\"6.9\",\"vulnerabilityTitle\":\"SSL - la vérification de signature a manqué signature d'Allowed\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-90043\",\"cveIds\":\"\",\"cvssBaseScore\":\"7.3\",\"cvssTemporalScore\":\"6.3\",\"vulnerabilityTitle\":\"SMB de méthode de cryptage faible de Remote Desktop Protocol de Vulnerability\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-90882\",\"cveIds\":\"\",\"cvssBaseScore\":\"4.7\",\"cvssTemporalScore\":\"4\",\"vulnerabilityTitle\":\"Windows désactivée ou PME signant pas l'utilisation de Required\",\"vulnerabilityVendor\":\"Qualys\"}","{\"vulnerabilityId\":\"QID-38601\",\"cveIds\":\"CVE-2013-2566,CVE-2015-2808,\",\"cvssBaseScore\":\"4.3\",\"cvssTemporalScore\":\"3.7\",\"vulnerabilityTitle\":\"SSL/TLS du chiffrement RC4 faible \ », \ « vulnerabilityVendor \ » : \ « Qualys \ « } »]}]
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaServiceMessageListener de 19:25:02,127 - : : : : : - VA : Sauvegardez au DB de contexte, lastscantime : 1467134394000, MAC : C0:4A:00:14:8D:4B
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaAdminServiceContext de 19:25:02,268 - : : : : : - VA : envoi du json élastique de recherche au PRI-réseau local
2016-06-28 DEBUG [pool-311-thread-8][] va.runtime.admin.vaservice.VaPanRemotingHandler de 19:25:02,272 - : : : : : - VA : Enregistré à la recherche élastique : Vulnérabilité d'exécution de code distant de Windows Remote Desktop Protocol de {C0:4A:00:14:8D:4B=[{"vulnerabilityId":"QID-90783","cveIds":"CVE-2012-0002,CVE-2012-0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft (MS12-020)","vulnerabilityVendor":"Qualys"}, certificat {"vulnerabilityId":"QID-38173","cveIds":"","cvssBaseScore":"9.4","cvssTemporalScore":"6.9","vulnerabilityTitle":"SSL - la vérification de signature a manqué vulnérabilité », « vulnerabilityVendor » : « Qualys »}, méthode de cryptage faible {"vulnerabilityId":"QID-90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows Remote Desktop Protocol a laissé », « vulnerabilityVendor » : « Qualys »}, signature {"vulnerabilityId":"QID-90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB désactivée ou PME signant non requis », « vulnerabilityVendor » : « Qualys »}, utilisation de {"vulnerabilityId":"QID-38601","cveIds":"CVE-2013-2566,CVE-2015-2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLS du chiffrement RC4 faible », « vulnerabilityVendor » : « Qualys »}]}

Logs à vérifier - vaservice.log. Vous pouvez le suivre directement d'ISE CLI :

```
Queue de vaservice.log d'application de show logging ISE21-3ek/admin#
```

Demande d'estimation de vulnérabilité à l'adaptateur

2016-06-28 DEBUG [endpointPollerScheduler-3][] cpm.va.service.util.VaServiceUtil de 17:07:13,200 - : : : : : - systemMsg VA SendSyslog : Service d'estimation [{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-NAC.ServiceName","Vulnerability », « TC-NAC.Status », « demande VA à l'adaptateur », « TC-NAC.Details », « demande VA à l'adaptateur pour le 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 vérifie chaque 5 minute le statut du balayage, jusqu'à ce qu'il soit de finition.

2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:09:43,459 - : : : : : - message d'adaptateur : le
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number des points finaux s'est
aligné pour vérifier des résultats de balayage : 1, nombre de points finaux alignés pour le
balayage : 0, le nombre de points finaux pour lesquels le balayage est en cours : 0"}
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:14:43,760 - : : : : : - message d'adaptateur : le
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number des points finaux s'est
aligné pour vérifier des résultats de balayage : 0, nombre de points finaux alignés pour le
balayage : 0, le nombre de points finaux pour lesquels le balayage est en cours : 1"}
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:19:43,837 - : : : : : - message d'adaptateur : le
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number des points finaux s'est
aligné pour vérifier des résultats de balayage : 0, nombre de points finaux alignés pour le
balayage : 0, le nombre de points finaux pour lesquels le balayage est en cours : 1"}
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:24:43,867 - : : : : : - message d'adaptateur : le
{"AdapterInstanceName":"QUALYS_VA","AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-
627f30248ad0","VendorName":"Qualys","OperationMessageText":"Number des points finaux s'est
aligné pour vérifier des résultats de balayage : 0, nombre de points finaux alignés pour le
balayage : 0, le nombre de points finaux pour lesquels le balayage est en cours : 1"}

L'adaptateur est fait avancer QID, des CVE les scores CVSS

2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 17:24:57,556 - : : : : : - message d'adaptateur : Certificat de
{"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 -
La vérification de signature a manqué signature de
Vulnerability","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90043","cveIds":"","cvssBaseScore":"7.3","cvssTemporalScore":"6.3","vulnerabilityTitle":"SMB
désactivée ou PME signant pas la vulnérabilité d'exécution de code distant de Windows Remote
Desktop Protocol de Required","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90783","cveIds":"CVE-2012-0002,CVE-2012-
0152,","cvssBaseScore":"9.3","cvssTemporalScore":"7.7","vulnerabilityTitle":"Microsoft
(l'utilisation de MS12-020)","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
38601","cveIds":"CVE-2013-2566,CVE-2015-
2808,","cvssBaseScore":"4.3","cvssTemporalScore":"3.7","vulnerabilityTitle":"SSL/TLS de la
méthode de cryptage faible faible de Remote Desktop Protocol du
cipher","vulnerabilityVendor":"Qualys"},{"vulnerabilityId":"QID-
90882","cveIds":"","cvssBaseScore":"4.7","cvssTemporalScore":"4","vulnerabilityTitle":"Windows
RC4 a laissé », « vulnerabilityVendor » : « Qualys »}]}
2016-06-28 les INFORMATIONS [SimpleAsyncTaskExecutor-
2][] cpm.va.service.processor.AdapterMessageListener de 17:25:01,282 - : : : : : - les détails
de point final envoyés aux forces de réaction immédiate est
{"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 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil de 17:25:01,853
- : : : : : - systemMsg VA SendSyslog : Le service d'estimation
[{"systemMsg":"91019","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability », « TC-NAC.Status », « VA s'est avec succès terminé », « TC-

NAC.Details », « VA terminé ; nombre de vulnérabilités trouvées : 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"]}]

Questions typiques

La question 1. ISE obtient l'état de vulnérabilité avec CVSS_Base_Score de 0.0 et CVSS_Temporal_Score de 0.0, alors que l'état de nuage de Qualys contient des vulnérabilités détectées.

Problème :

Tout en vérifiant l'état du nuage de Qualys vous pouvez voir des vulnérabilités détectées, toutefois sur ISE vous ne les voyez pas.

Debugs vus dans vaservice.log :

```
2016-06-02 les INFORMATIONS [SimpleAsyncTaskExecutor-
2][] cpm.va.service.processor.AdapterMessageListener de 08:30:10,323 - : : : : : - les détails
de point final envoyés aux forces de réaction immédiate est
{"C0:4A:00:15:75:C8":[{"vulnerability":{"CVSS_Base_Score":0.0,"CVSS_Temporal_Score":0.0},"time-
stamp":1464855905000,"title":"Vulnerability","vendor":"Qualys"}]}
```

Solution :

La raison pour le score de cvss étant zéro est l'un ou l'autre qu'elle n'a aucune vulnérabilité ou le marquage de cvss n'a pas été activé en nuage de Qualys avant que vous configuriez l'adaptateur par UI. La base de connaissances contenant des cvss marquant la fonction activée est téléchargée après que l'adaptateur soit configuré première fois. Vous devez s'assurer que le marquage CVSS a été activé avant, exemple d'adaptateur avez été créé sur ISE. Il peut être fait sous la Gestion > les états de vulnérabilité > installé > CVSS > marquage de l'enable CVSS

La question 2. ISE ne récupère pas des résultats du nuage de Qualys, quoique la stratégie correcte d'autorisation ait été frappée.

Problème :

La stratégie corrigée d'autorisation a été appariée, qui devrait déclencher le balayage VA. En dépit de ce fait aucun balayage n'est fait.

Debugs vus dans vaservice.log :

```
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 16:19:15,401 - : : : : : - message d'adaptateur :
(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 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 16:19:15,401 - : : : : : - message d'adaptateur :
{"requestedMacAddress":"24:77:03:3D:CF:20","scanStatus":"SCAN_ERROR","scanStatusMessage":"Error
déclenchant le balayage : Erreur tandis que code et erreur de balayage de trigeringon-exigence
comme suit 1904 : rien l'IPS spécifié est habilité à la Gestion
scanning.","lastScanTimeLong":0,"ipAddress":"10.201.228.102"} de vulnérabilité
```

```
2016-06-28 DEBUG [SimpleAsyncTaskExecutor-2][] cpm.va.service.processor.AdapterMessageListener
de 16:19:15,771 - : : : : : - le résultat de balayage d'adaptateur a manqué pour
Macaddress:24:77:03:3D:CF:20, IP Address(DB) : 10.201.228.102, plaçant l'état à manqué
2016-06-28 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil de 16:19:16,336
- : : : : : - systemMsg VA SendSyslog : Service d'estimation
[{"systemMsg":"91008","isAutoInsertSelfAcsInstance":true,"attributes":["TC-
NAC.ServiceName","Vulnerability », « TC-NAC.Status », « panne VA », « TC-NAC.Details », « erreur
déclenchant le balayage : Erreur tandis que code et erreur de balayage sur demande trigering
comme suit 1904 : rien l'IPS spécifié est habilité au 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"]}] de Gestion de vulnérabilité
```

Solution :

Le nuage de Qualys indique que l'IP address du point final n'est pas habilité à la lecture, s'assurent s'il vous plaît que vous avez ajouté l'IP address du point final à la Gestion de vulnérabilité > aux ressources > aux ressources en hôte > nouveau > les hôtes dépistés par IP

Références

- Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.1
- Support et documentation techniques - Cisco Systems
- Vidéo : ISE 2.1 avec Qualys
- Documentation de Qualys