

## 1. Security Technical Implementation Guide - STIG

Les STIG sont des méthodologies de cybersécurité pour la standardisation de la sécurité dans les systèmes d'information. Ils vont des équipements réseau, aux ordinateurs (serveur et PC), en passant par des applications. De manière générale, le but des STIG est d'augmenter la sécurité de l'ensemble de l'infrastructure en réduisant le nombre de vulnérabilités. La liste de l'ensemble des STIG est disponible sur <https://www.stigviewer.com/stigs>. Pour la partie VMware voici ce qui est couvert par les STIG.

VMware ESX 3 Policy

VMware ESX 3 Server

VMware ESX 3 Virtual Center

VMware ESX 3 Virtual Machine

VMware ESXi Server 5.0

VMware ESXi Version 5 Virtual Machine

VMware ESXi v5

VMware NSX Distributed Firewall

VMware NSX Distributed Logical Router

VMware NSX Manager

VMware vCenter Server

VMware vCenter Server Version 5

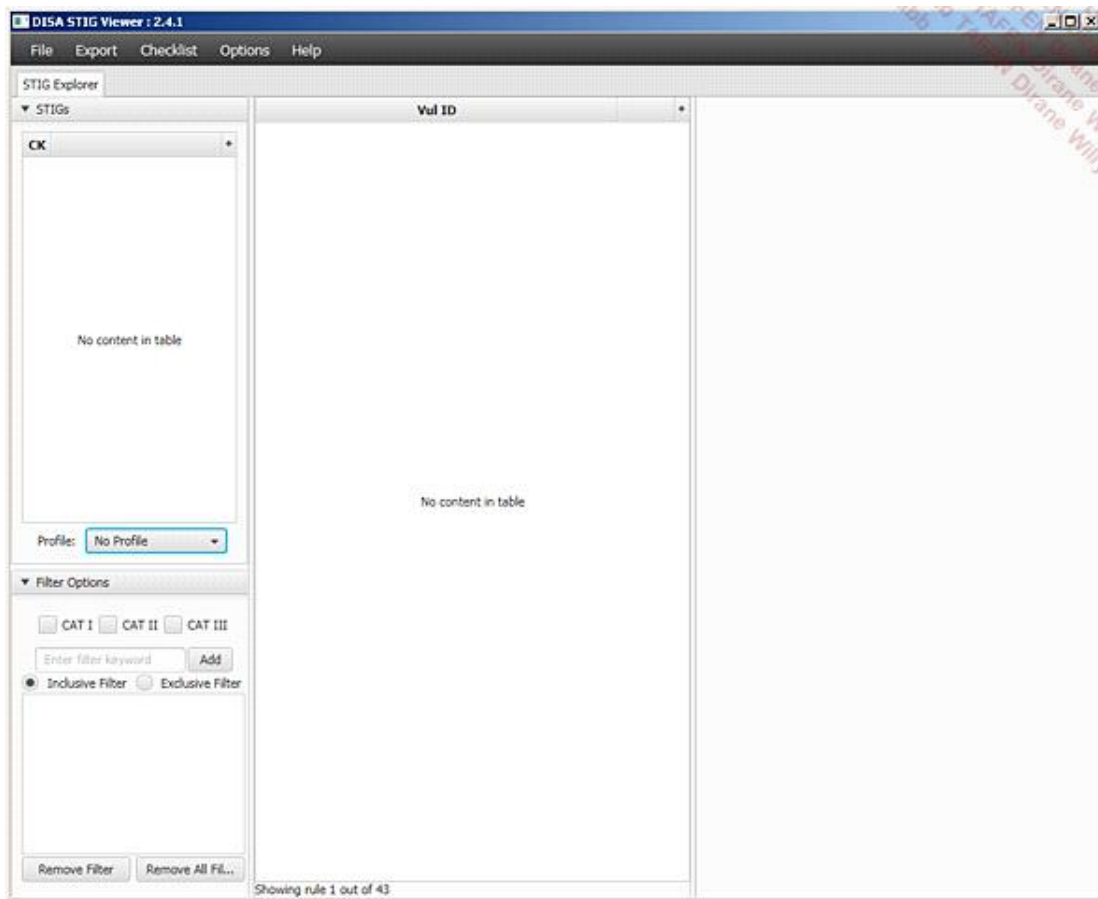
VMware vSphere ESXi 6.0

VMware vSphere Virtual Machine Version 6

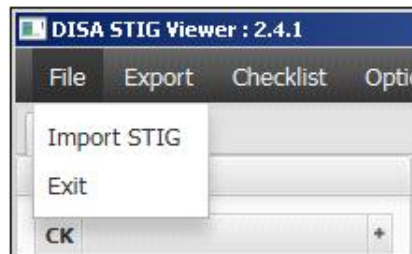
VMware vSphere vCenter Server Version 6

Un fichier STIG est disponible sous différentes formes Excel, JSON ou XML, si nous les téléchargeons depuis le site [stigviewer.com](http://stigviewer.com). Dans le cas où nous les téléchargeons depuis le site de l'Information Assurance Support Environnement (<http://iase.disa.mil/stigs/Pages/a-z.aspx>) (IASE) les fichiers seront au format ZIP.

Il existe un lecteur pour les STIG, le STIGViewer (<http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx>), il nécessite d'avoir Java pour l'utiliser car il s'agit d'un fichier de type JAR. Lancez le fichier JAR.



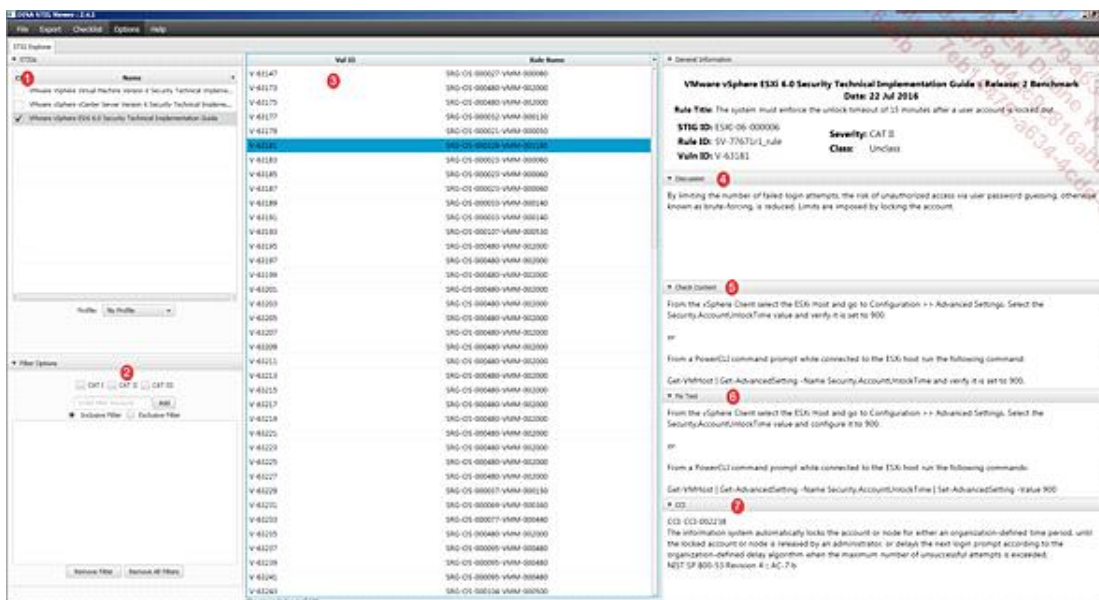
Importez le(s) fichier(s) STIG(s).



Sélectionnez l'ensemble des fichiers à importer.

	U_VMware_vSphere_6-0_Virtual_Machine_VIR1_STIG(1).zip	1/22/2017 6:12 PM	WinRAR ZIP archive	261 KB
	U_VMware_vSphere_6-0_vCenter_Server_for_Windows_VIR2_STIG.zip	1/22/2017 6:12 PM	WinRAR ZIP archive	306 KB
	U_VMware_vSphere_6-0_VIR1_Overview(1).zip	1/22/2017 6:12 PM	WinRAR ZIP archive	85 KB
	U_VMware_vSphere_6-0_ESX_VIR2_Manual_STIG.zip	1/22/2017 6:12 PM	WinRAR ZIP archive	340 KB

Une fois importé, vous pouvez choisir avec quel STIG travailler (1), puis le critère de criticité (2) ce qui permet créer un filtre automatique dans la liste des règles de sécurisation (3). Les points (4), (5), (6) et (7) correspondent respectivement à la raison de la sécurisation (4), comment faire pour vérifier (5) et remédier (6) le paramètre, et à quelle règle des standards de sécurité du NIST la recommandation correspond (7).



## 2. Runecast

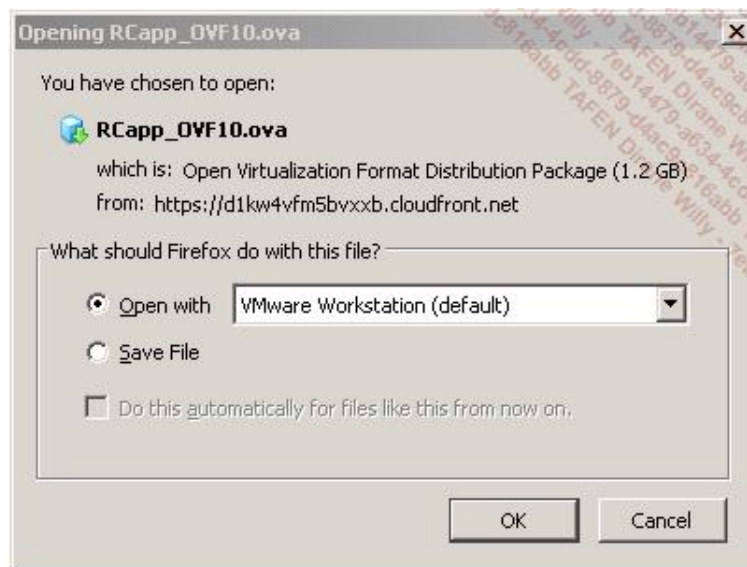
Runecast s'appuie sur les Best Practice, la base de connaissance de VMware (KB), les guides de sécurisation afin de faire un audit de la plateforme VMware. À l'heure actuelle, il ne met pas en place les actions correctives à mener. Avec la version 1.5, qui est disponible depuis le 7 mars 2017, Runecast supporte plusieurs serveurs vCenter simultanément.

Ceci n'est pas un guide d'utilisation, mais cette présentation permettra de découvrir les possibilités du produit et de l'appréhender. Nous ne parlons pas des prérequis d'ouverture de flux ni des droits utilisateurs pour faire l'inventaire. Ces informations sont disponibles dans le guide de l'utilisateur.

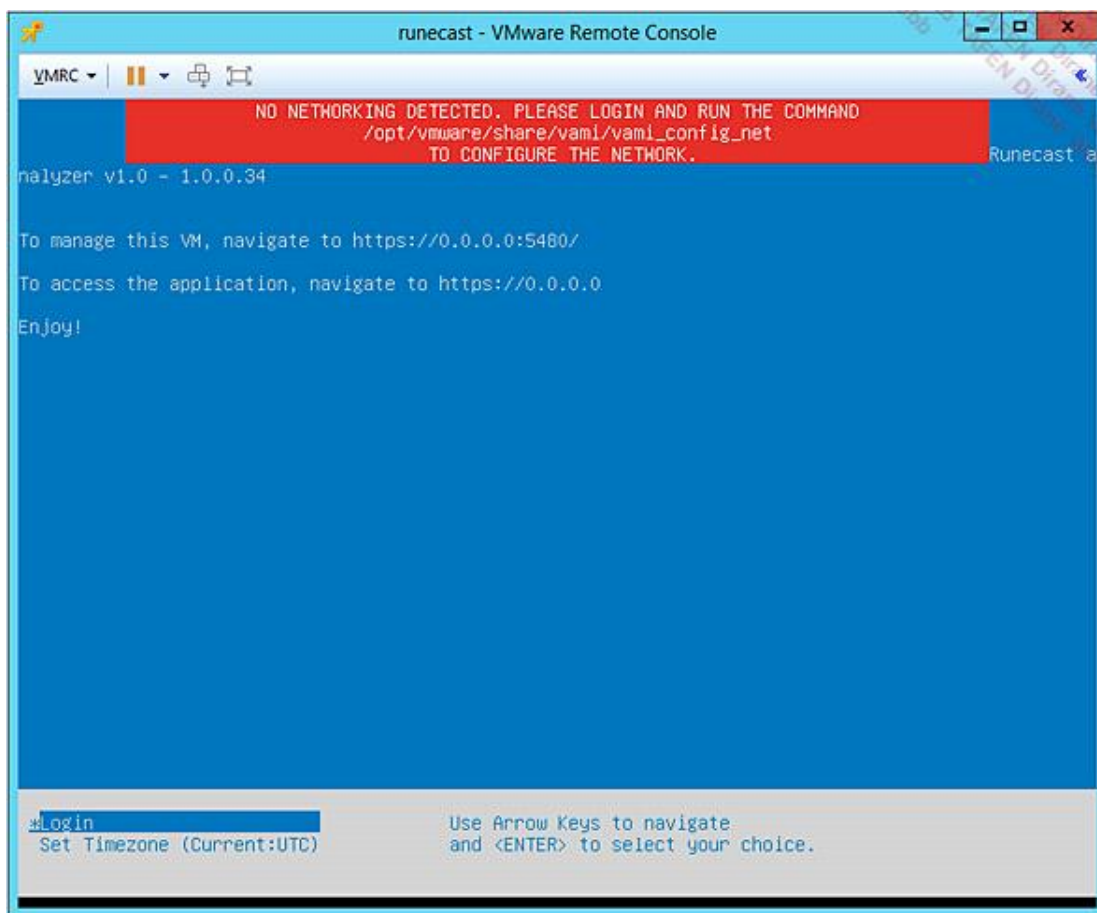
Il suffit d'aller sur leur site <https://www.runecast.biz> et de télécharger la version gratuite. L'application est disponible sous la forme d'un OVA de 1.2 Go (1), et la mise à jour de l'appliance sous forme de fichier ISO de 60 Mo (2) au moment de l'écriture de cet ouvrage.



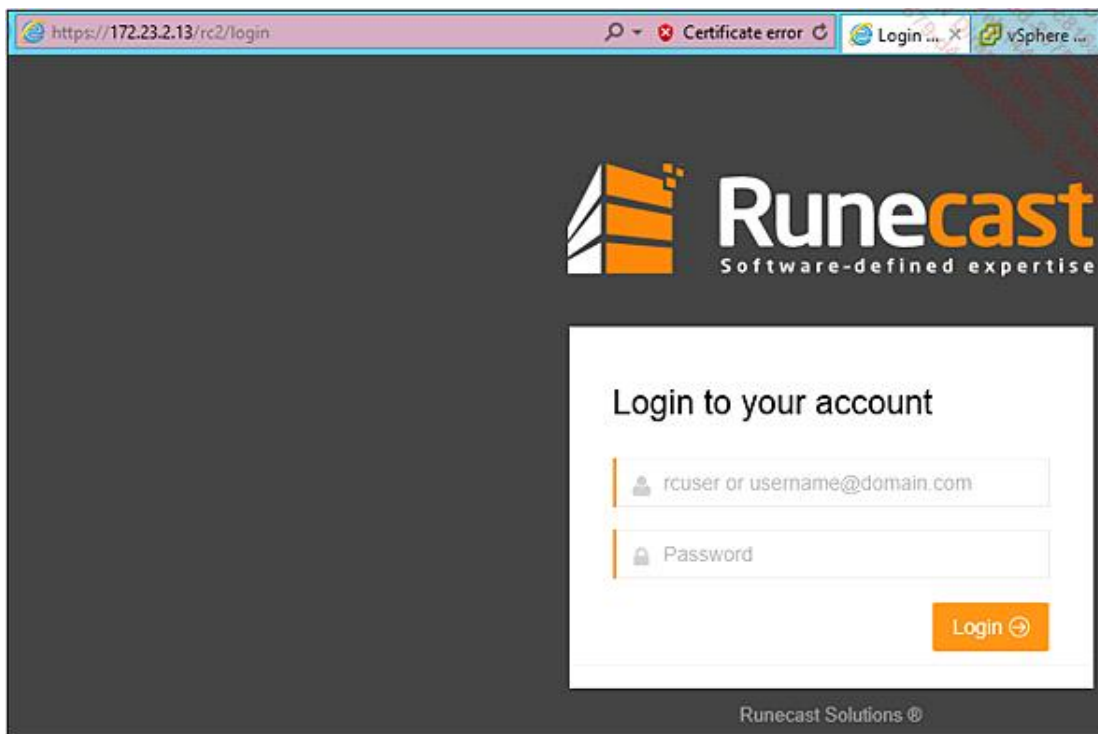
Sauvegardez le fichier.



Ici nous allons nous concentrer sur la partie installation et configuration de Runecast. Importez l'OVA dans l'environnement VMware et compléter les informations nécessaires (IP, nom de la machine, etc.). Une fois la machine virtuelle lancée et prête à être utilisée, connectez-vous en mode console. Cela permet de voir que l'installation s'est effectuée correctement. Dans le cas contraire, vous aurez le retour suivant :



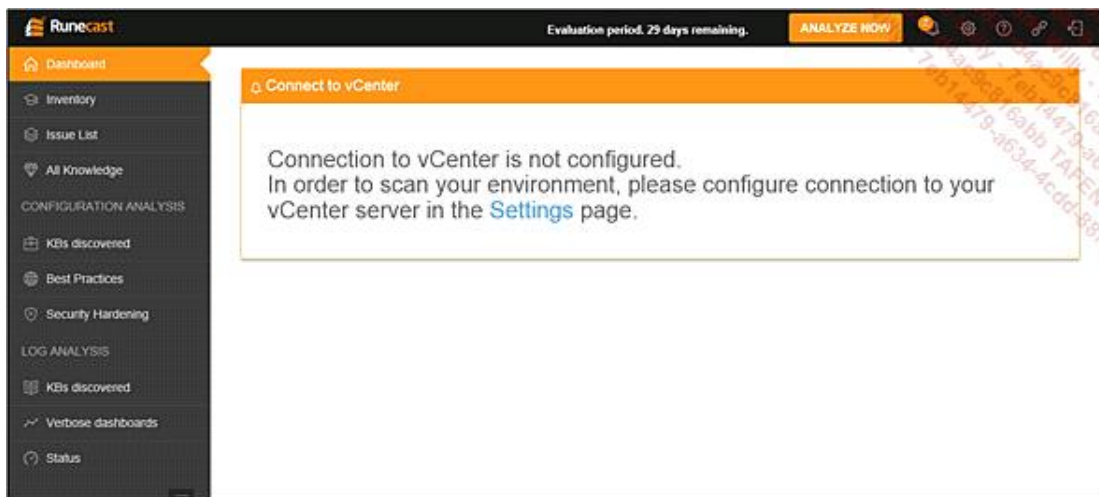
Pour lancer le script `/opt/vmware/share/vami/vami_config_net` ne pas oublier d'utiliser `sudo` sinon vous ne pourrez pas modifier la configuration. Une fois le problème corrigé, vous pouvez vous connecter à l'application.



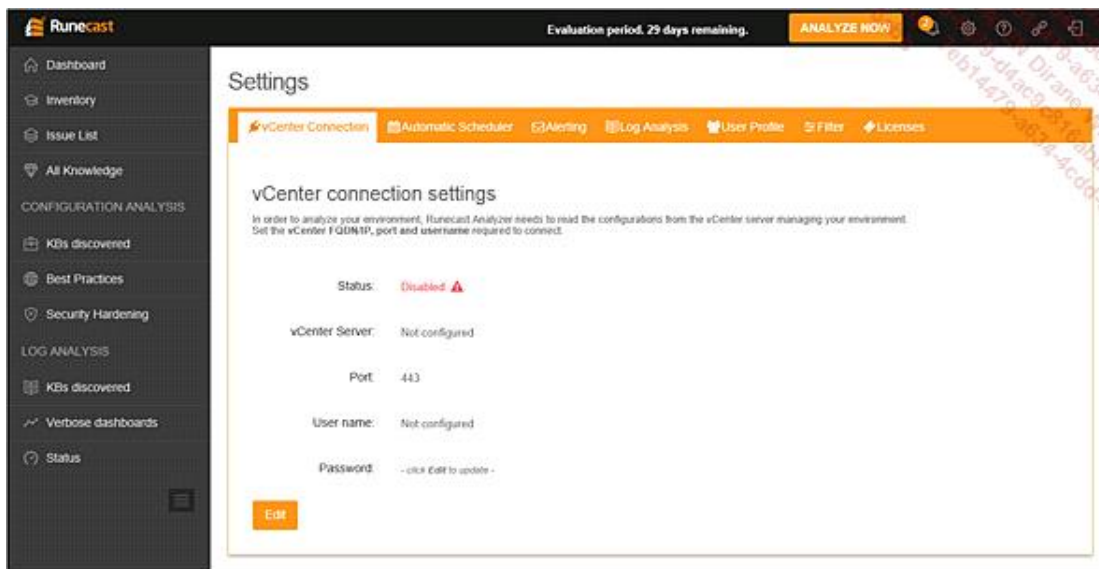
Le compte utilisateur est **rcuser** et son mot de passe se trouve dans le fichier user guide.

Une fois connecté, la première étape est de configurer l'environnement. Pour cela, vous pouvez :

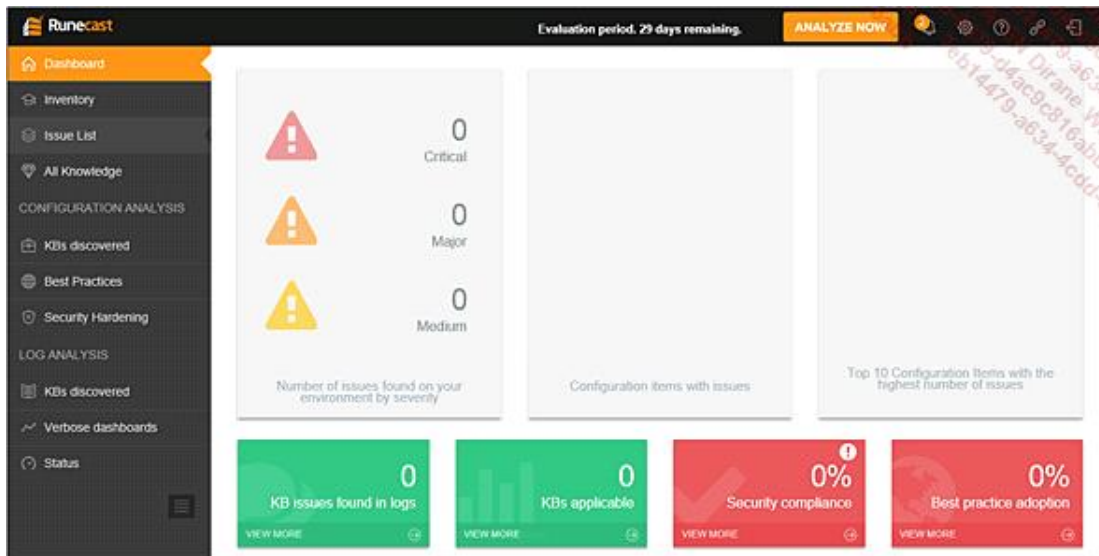
- Soit cliquer sur **Settings**.
- Soit cliquer sur la roue crantée en haut à droite.



Le premier onglet est celui concernant la connexion au vCenter : **vCenter Connection**.

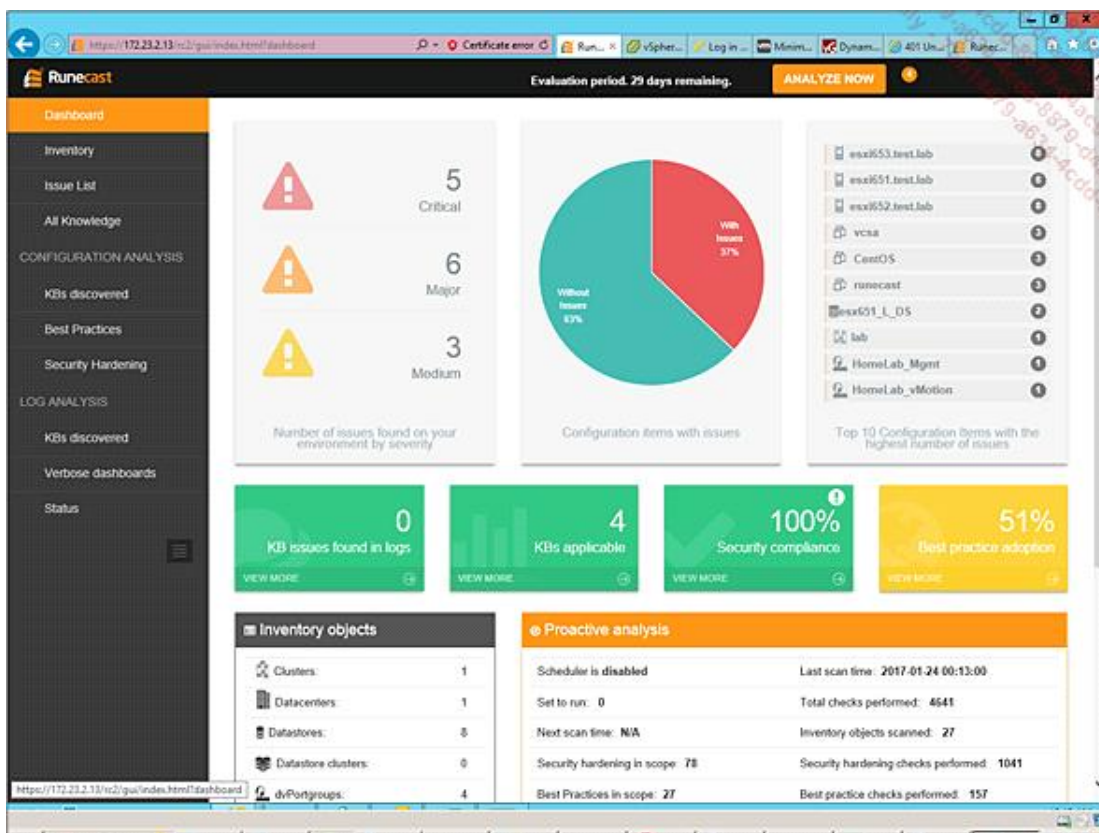


Remplissez les champs **vCenter Server**, **username** et **password**. Puis allez dans le **Dashboard**.



Il est vide (ce qui est normal). Cliquez sur **ANALYZE NOW**. Ici, l'opération a été assez rapide, il faut savoir que le lab contient 3 ESXi, 1 vCenter, 3 machines virtuelles et 3 types de stockage (Local, iSCSI, NFS).





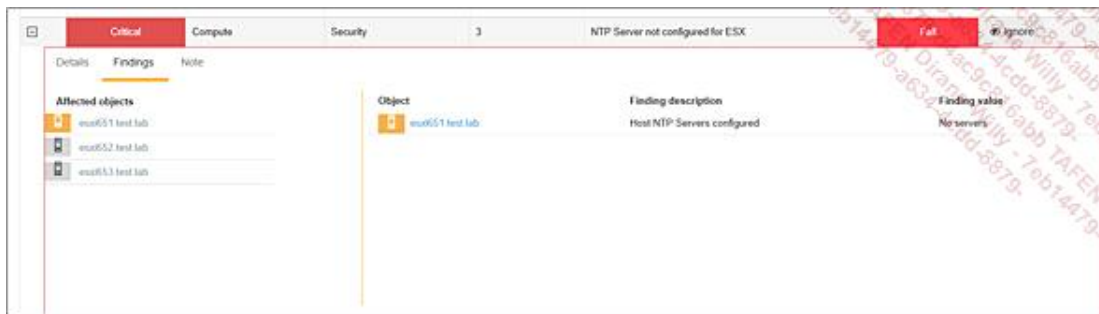
La même vue après l'analyse. Vous voyez en un coup d'œil que l'application des meilleures pratiques (« best practices ») est quelque peu oubliée. Il suffit de cliquer sur l'application des **Best Practice** pour avoir la liste des règles qui ne sont pas appliquées.

Severity	Applies To	Affects	Objects	Description	Result	Action
Critical	Compute	Security	3	NTP Server not configured for ESX	Fail	Ignore
Critical	Compute	Security	3	NTP Server not running in ESX	Fail	Ignore
Critical	Compute	Security	1	Remote TSM is enabled	Fail	Ignore
Critical	Compute	Security	3	Networking for ESX host set to accept MAC address changes	Fail	Ignore
Critical	Compute	Security	3	Networking for ESX host set to accept forged transcripts	Fail	Ignore
Critical	Compute	Security	0	Host SSL certificate expiration date	Pass	Ignore
Major	Compute	Availability	4	Port group does not have redundant NIC	Fail	Ignore
Major	Compute	Security	3	TSM Timeout not set	Fail	Ignore
Major	VM	Security	2	RemoteDisplay maxConnection VM setting not set to 1	Fail	Ignore
Major	Storage	Manageability	1	Datastore has less than 10% free space	Fail	Ignore
Major	Compute	Availability	1	No alternate isolation address specified for the HA cluster	Fail	Ignore
Major	Compute	Performance	3	Non recommended Hyperthreading configuration for ESX host	Fail	Ignore
Major	Compute	Performance	0	CPU Speeds are inconsistent across ESX in cluster	Pass	Ignore

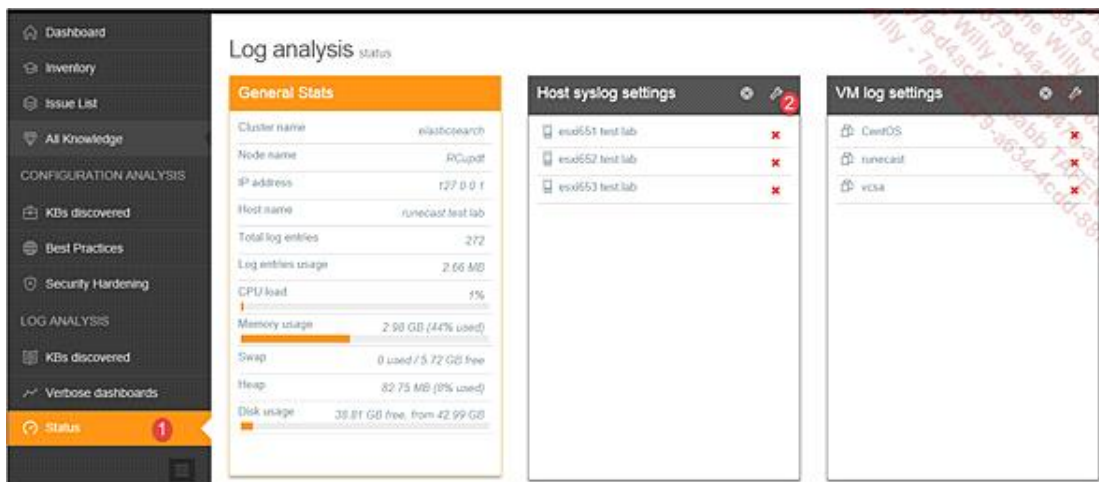
En cliquant sur une ligne, vous avez en détail l'explication sur le point qui n'a pas passé avec succès le test.



Dans la section **Findings**, vous savez quels composants de l'infrastructure doivent être corrigés.






Vous devez aussi configurer la gestion des logs pour les serveurs ESXi et machines virtuelles. Pour cela, cliquez sur **Status**, puis sur la clé à molette pour la gestion du Syslog des serveurs ESXi.



Cochez les serveurs pour lesquels vous souhaitez configurer le syslog, puis cliquez sur **Configure**.



### Configure Hosts

 esxi651.test.lab	<input checked="" type="checkbox"/>
 esxi652.test.lab	<input checked="" type="checkbox"/>
 esxi653.test.lab	<input checked="" type="checkbox"/>

Click "Configure" to enable logging on ☐ hosts and disable logging on ☒ hosts.

Confirmez l'opération.

### Please confirm configuration changes

**Hosts listed below will be configured to send logs to Runecast appliance, following actions will be performed:**

1. Runecast appliance address "udp://172.23.2.13:514" will be added as loghost (Syslog.global.logHost), or appended to the list if there is other loghost configured
2. Firewall setting for syslog service will be enabled, if not enabled already for other syslog collectors
3. Syslog configuration will be refreshed (system.syslog.reload() )

☒ esxi651.test.lab  
☒ esxi652.test.lab  
☒ esxi653.test.lab

Répétez les mêmes étapes pour la gestion des logs des machines virtuelles.

Après plusieurs heures, vous commencez à avoir les premières remontées d'erreurs.

