Amazon Inspector

Julien Simon
Principal Technical Evangelist, AWS
julsimon@amazon.fr
@julsimon

amazon web services

Agenda

Qu'est-ce qu'Inspector peut faire pour vous ?

Disponibilité et tarification

Installation

Démonstration

Conseils et ressources

Questions et réponses

Amazon Inspector

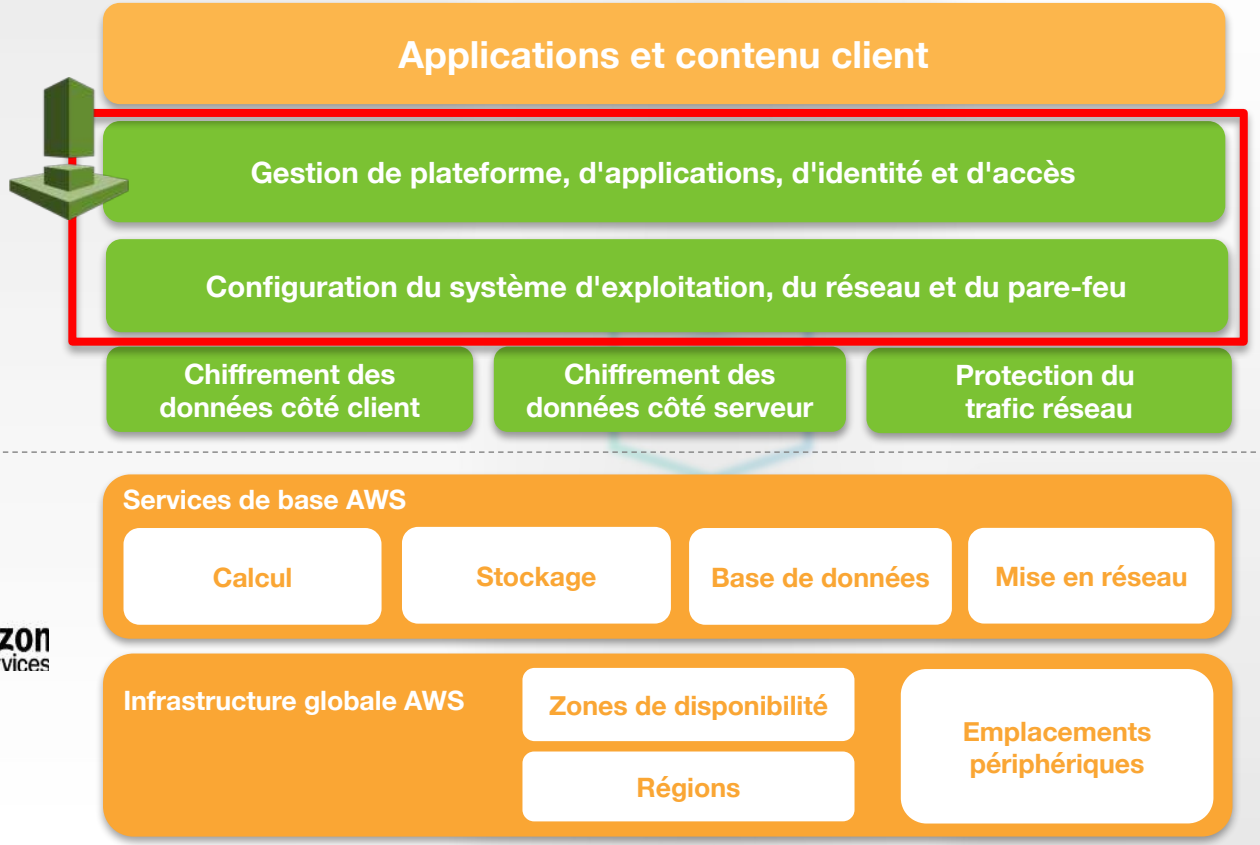
Inspector vous permet d'analyser vos instances EC2 et d'identifier des failles de sécurité.

1. Définissez la liste des instances avec un *tag*
2. Déployez l'agent Inspector sur les instances concernées
3. Lancez une évaluation, basée sur une liste de règles pré-établie.
4. Analysez les résultats.

Note : Inspector ne change rien au modèle de sécurité partagée.

https://aws.amazon.com/inspector/

AWS Inspector vous aide à sécuriser votre plate-forme



Vous devez définir vos contrôles **DANS** le cloud

AWS se charge de la sécurité **DU** cloud

amazon web services

Terminologie Inspector

Evaluation (*Assessment*)

- Analyse d'une application afin de détecter les failles de sécurité

Cible d'évaluation (*Assessment Target*)

- Ensemble d'instances EC2 que vous voulez évaluer

Groupe de règles (*Rule Package*)

- Ensemble de vérifications de sécurité (« règles »)

Modèle d'évaluation (*Assessement Template*)

- Cible + groupe de règles + durée

Résultats (*Findings*)

- Problème de sécurité potentiel dans votre application
- Les données collectées lors de l'évaluation correspondent à une règle
- Description détaillée, contexte et étapes de résolution

Groupes de règles

- ***Common Vulnerabilities and Exposures***
  - Vulnérabilités CVE http://cve.mitre.org
  - https://s3-us-west-2.amazonaws.com/rules-engine/CVEList.txt (43,819)
- ***CIS Operating System Security Configuration Benchmarks***
  - Vulnérabilités du *Center for Internet Security* http://cisecurity.org
  - http://benchmarks.cisecurity.org
- ***Security Best Practices***
  - Bonnes pratiques SSH, mots de passe, etc. (Linux uniquement)
  - https://docs.aws.amazon.com/fr_fr/inspector/latest/userguide/inspector_security-best-practices.html
- ***Runtime Behavior Analysis***
  - Comportement des instances pendant l'évaluation (protocoles réseau, etc.)
  - https://docs.aws.amazon.com/fr_fr/inspector/latest/userguide/inspector_runtime-behavior-analysis.html

Disponibilité et prix

- Inspector est disponible dans les régions suivantes :
  - US: Oregon, N. Virginia
  - EU: Irlande
  - Asia Pacific: Corée du Sud, Inde, Japon, Australie

- Tarif dégressif : de $0.30 à $0.05 par évaluation

- Niveau d'usage gratuit : 250 évaluations pendant 90 jours

Agent Inspector – Linux

- Amazon Linux (>= 2015.03), Ubuntu (14.04 LTS), RHEL (7.2), CentOS (7.2)
- Versions de noyau Linux supportées :https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json

```
$ wget https://d1wk0tztpsntt1.cloudfront.net/linux/latest/install

$ sudo bash install

$ sudo /opt/aws/awsagent/bin/awsagent status

$ sudo /etc/init.d/awsagent [ stop | start ]
```

Attention : l'agent dépend du noyau. Il est prudent de le mettre à jour après chaque mise à jour du noyau

Agent Inspector – Windows

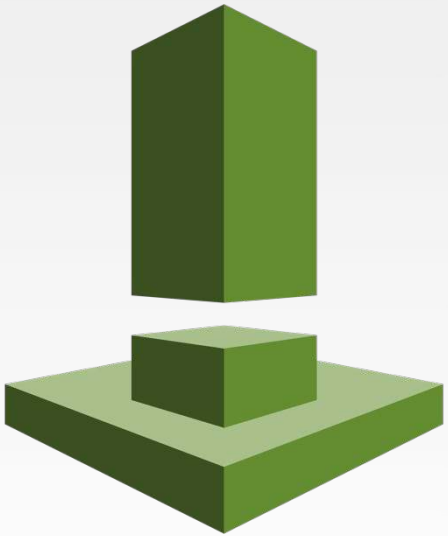
- Windows Server 2008 R2, Windows Server 2012 et 2012 R2
- Téléchargez et exécutez le fichier suivant :

  https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe
- Lancement et arrêt via *services.msc* :
  - *AWS Agent Service*
  - *AWS Agent Updater Service*

Utiliser Inspector

- Console AWS (uniquement en Anglais)
- Ligne de commande AWS https://docs.aws.amazon.com/cli/latest/reference/inspector/index.html
- SDK AWS https://aws.amazon.com/tools
  - Java https://docs.aws.amazon.com/AWSJavaSDK/latest/javadoc/com/amazonaws/services/inspector/AmazonInspector.html
  - Python https://boto3.readthedocs.org/en/latest/reference/services/inspector.html
  - Documentation de l'API https://docs.aws.amazon.com/inspector/latest/APIReference/Welcome.html

Démonstration



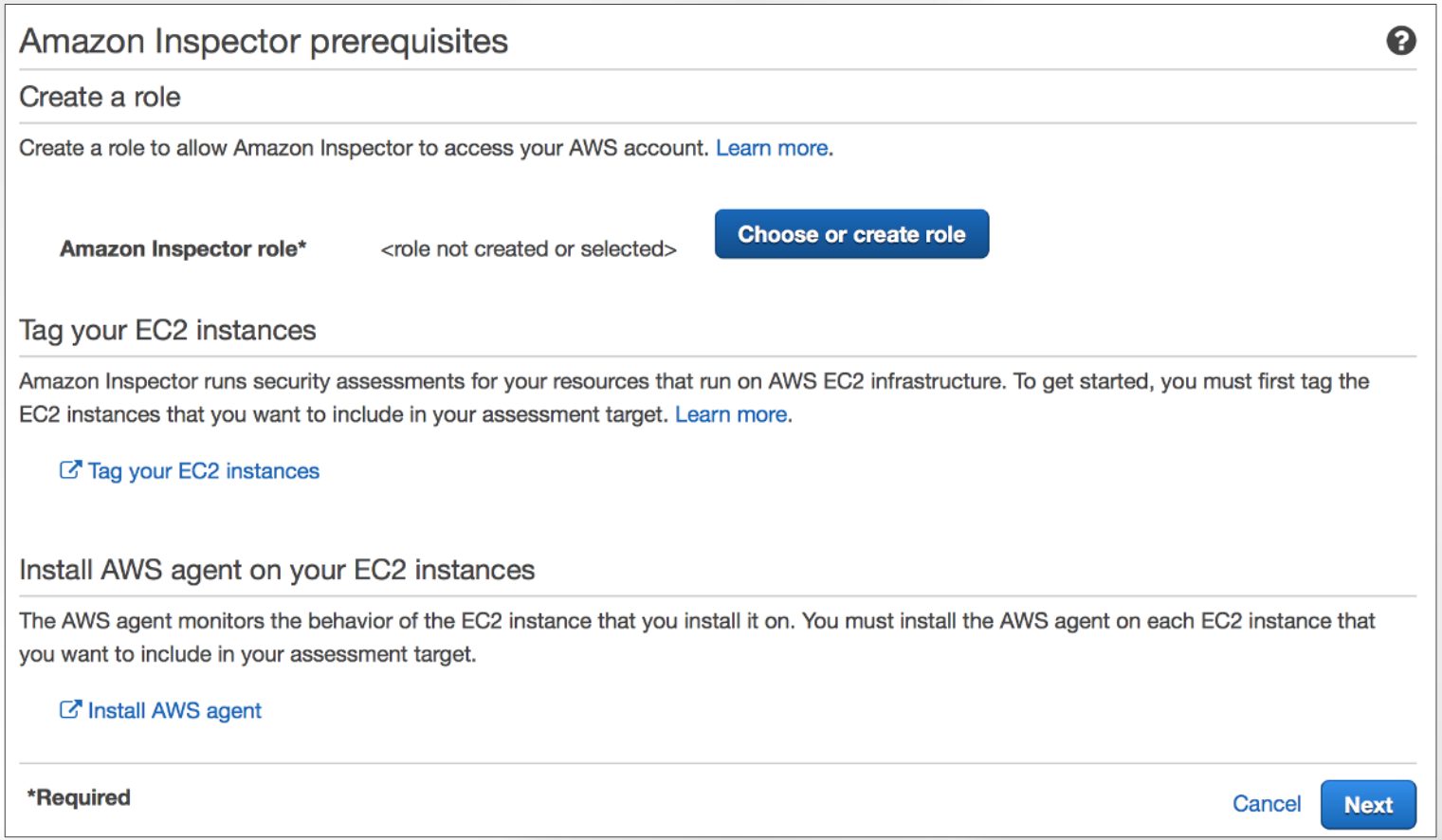
3 instances Linux

- Ubuntu 14.04.02 LTS (Avril 2014)
- Amazon Linux 2015.03
- Amazon Linux 2016.09

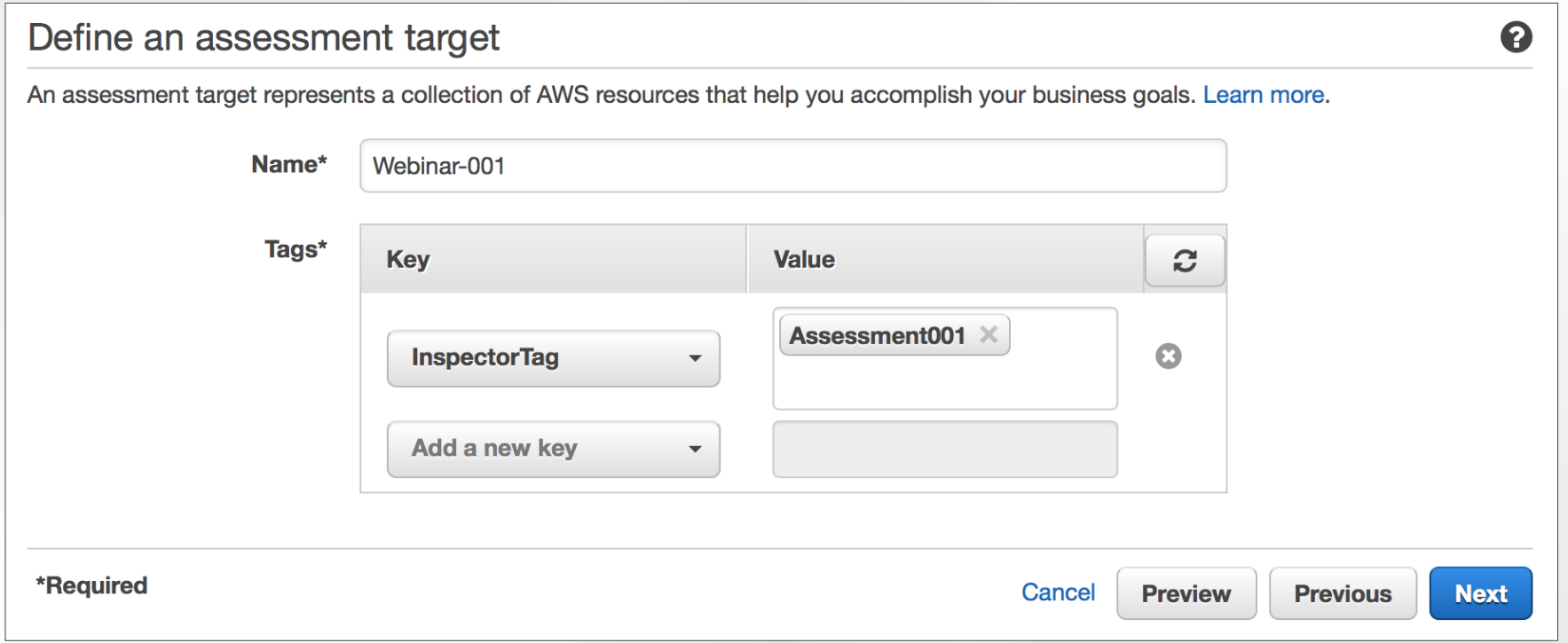
→ Packages PHP, MySQL, Java, Apache, Bind, etc.

1 instance Windows Server 2012

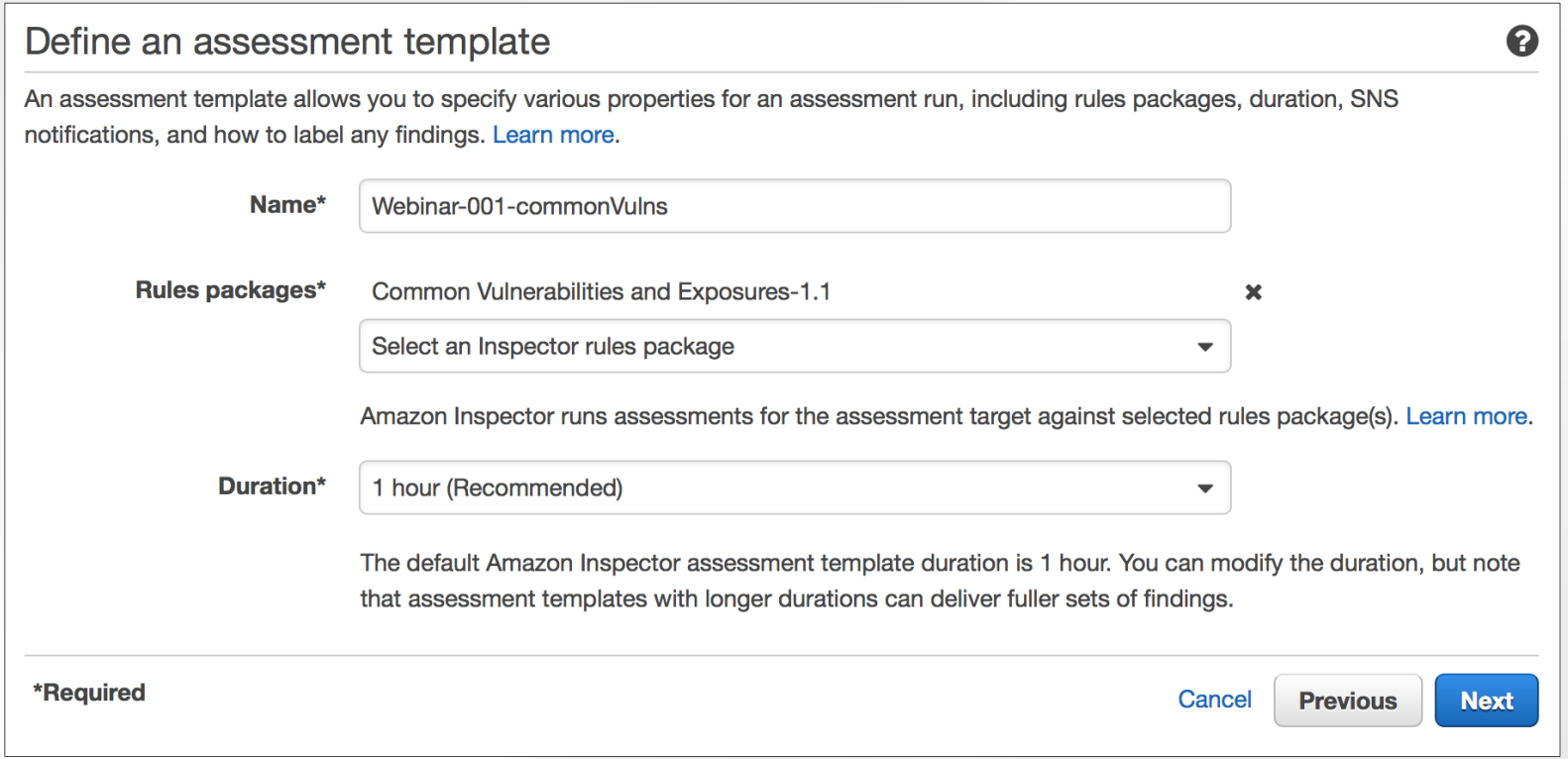
Pré-requis



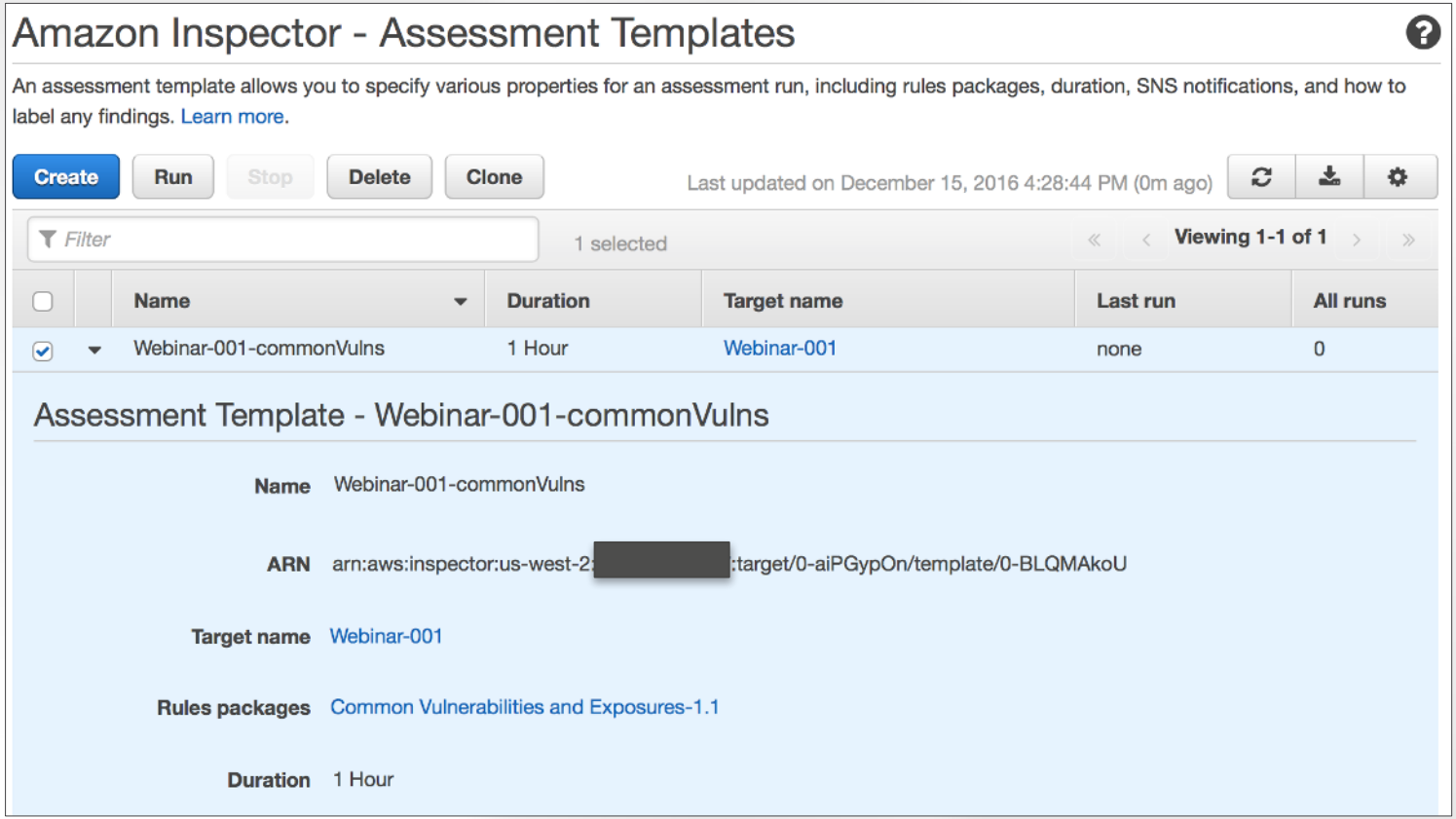
Définir une cible d'évaluation



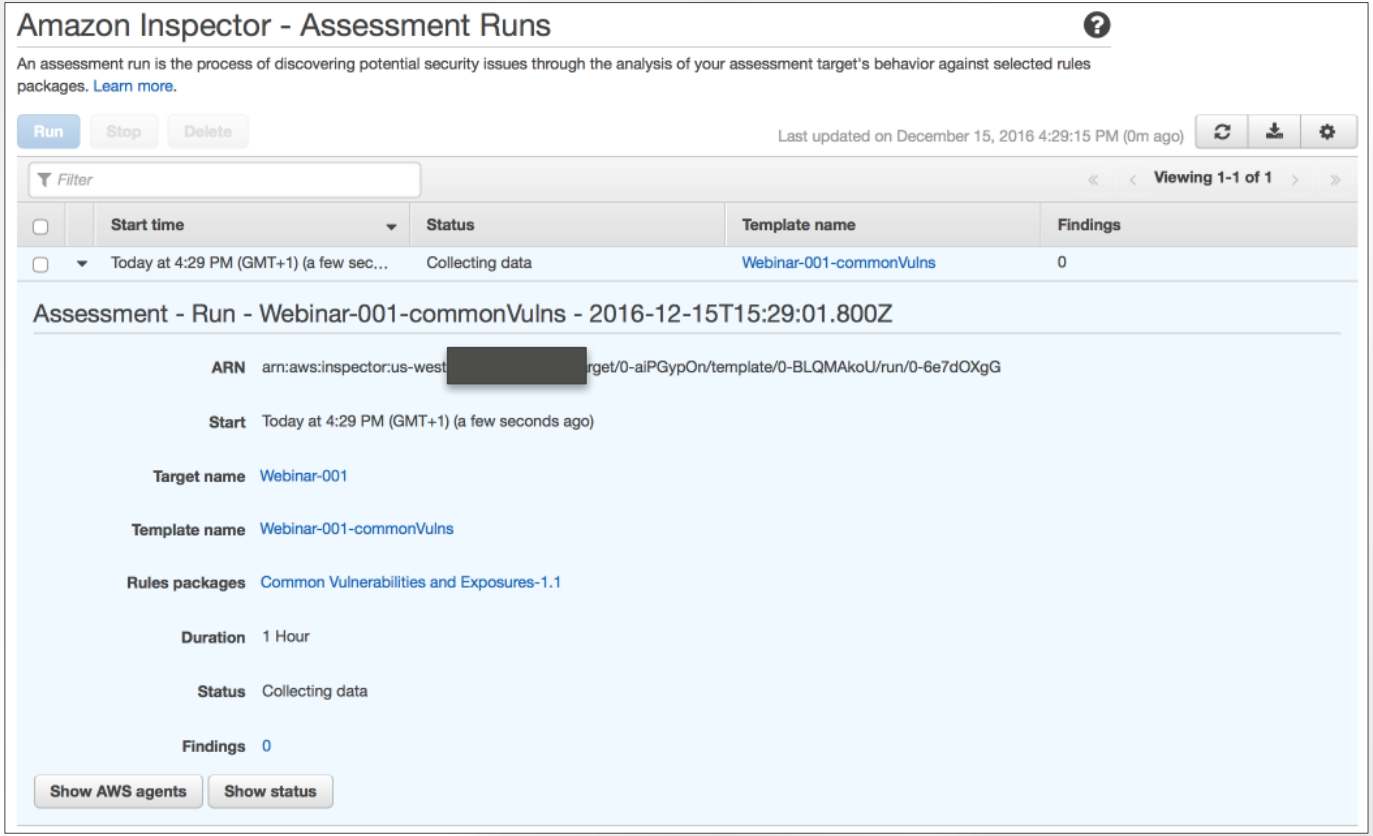
Définir un modèle d'évaluation



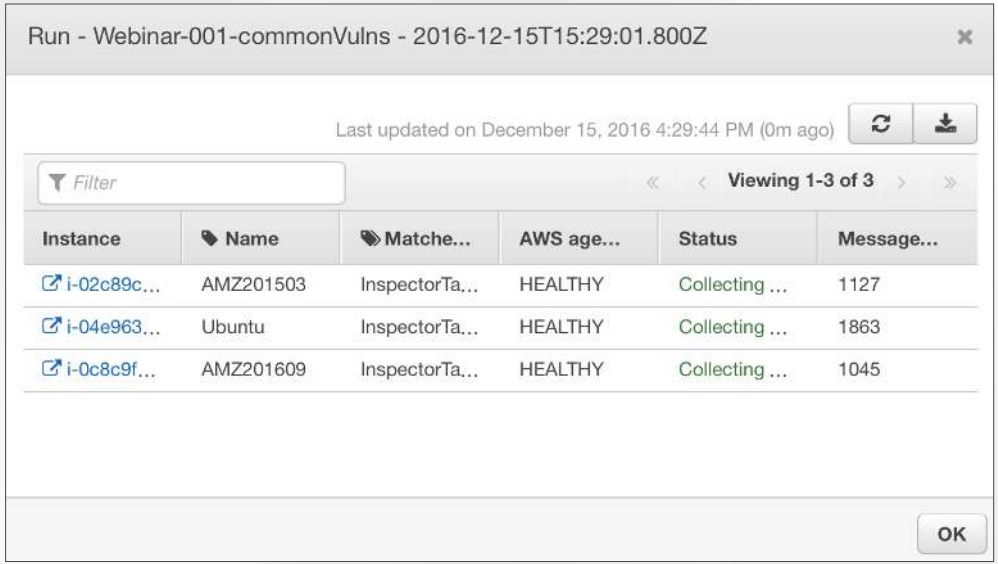
Récapitulatif du modèle d'évaluation

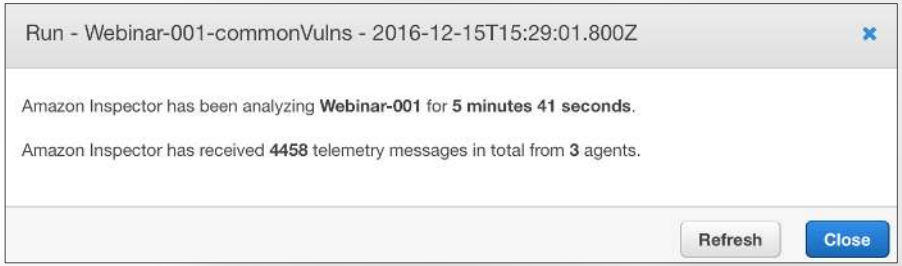


Lancer l'évaluation



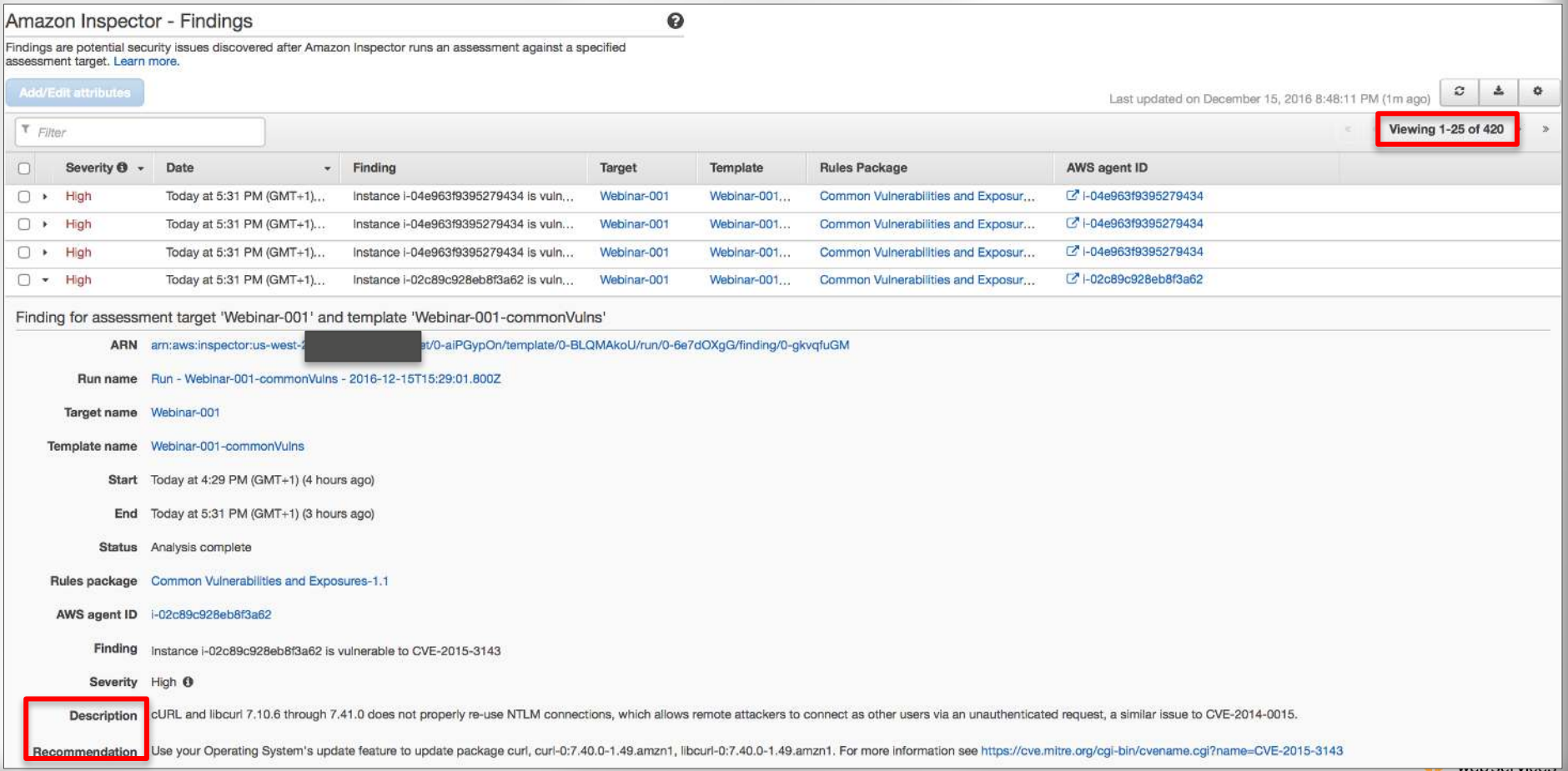
Pendant l'évaluation





amazon web services

Lister les résultats dans la console



Lister les résultats avec la ligne de commande AWS

```
$ aws inspector list-assessment-runs
{
    "assessmentRunArns": [
        "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGypOn/template/0-BLQMAkoU/run/0-
6e7dOXgG"
    ]
}

$ aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-
west-2:ACCOUNT:target/0-aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG”
…
    "findingArns": [
 "arn:aws:inspector:us-west-2:ACCOUNT:target/0-aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG/
finding/0-01Eg2UgO",
…

$ aws inspector describe-findings --finding-arns "arn:aws:inspector:us-
west-2:ACCOUNT:target/0-aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG/finding/0-01Eg2UgO"
```

Le résultat de notre évaluation

Ubuntu 14.04.02

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-
aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG" --filter '{"severities":["High"], "agentIds":
["i-04e963f9395279434"]}' --max-results 1000 --output text | grep FINDINGARNS | wc –l
242
```

Amazon Linux 2015.03

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-
aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG" --filter '{"severities":["High"], "agentIds":
["i-02c89c928eb8f3a62"]}' --max-results 1000 --output text | grep FINDINGARNS | wc –l
69
```

Amazon Linux 2016.09

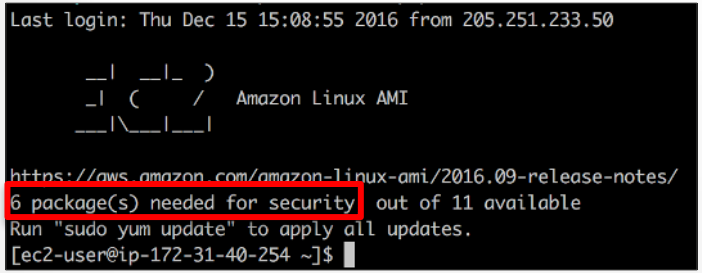
```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-
aiPGypOn/template/0-BLQMAkoU/run/0-6e7dOXgG" --filter '{"severities":["High"], "agentIds":
["i-0c8c9f709dd7f7cfd"]}' --max-results 1000 --output text | grep FINDINGARNS | wc –l
4
```

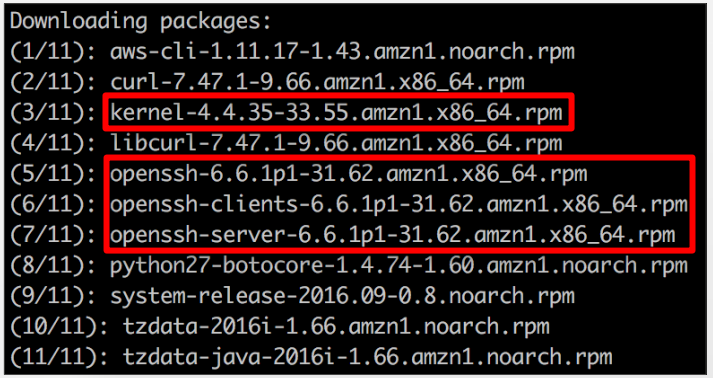
CVE-2015-8325 (OpenSSH)
CVE-2016-7039 / CVE-2016-8666 / CVE-2016-9083 (Linux kernel)

Comment corriger les problèmes ?

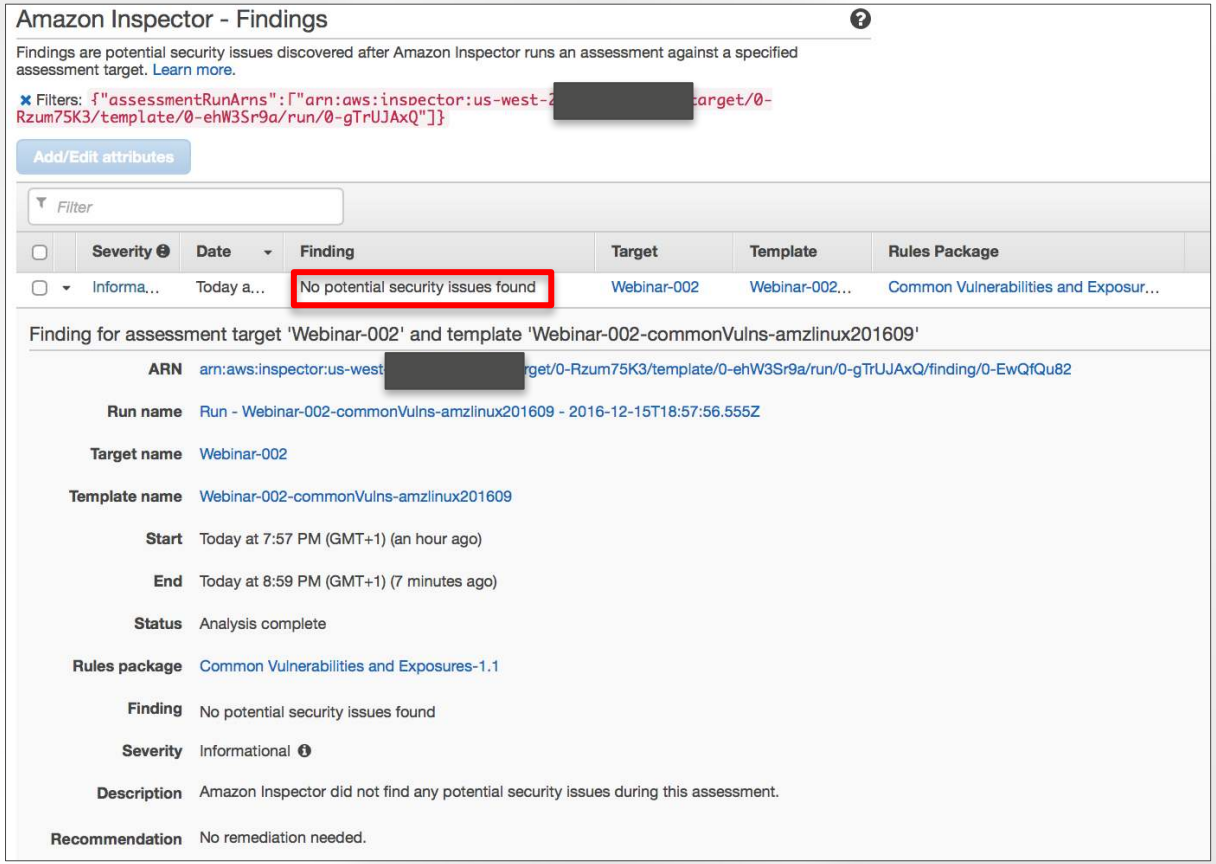
Mettez à jour vos instances régulièrement !

```
$ sudo yum update --cves=… -y

$ sudo yum update --security -y

$ sudo yum update -y
```





Evaluons à nouveau l'instance Amazon Linux 2016.09



Après mise à jour et scan de 24 heures ☺

Ubuntu 14.04.02

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-
aiPGypOn/template/0-KQ1FrZu6/run/0-Ixqaicyh" --filter '{"severities":["High"], "agentIds":
["i-04e963f9395279434"]}' --max-results 1000 --output text | grep FINDINGARNS | wc –l
52
```

Amazon Linux 2015.03

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-
aiPGypOn/template/0-KQ1FrZu6/run/0-Ixqaicyh" --filter '{"severities":["High"], "agentIds":
["i-02c89c928eb8f3a62"]}' --max-results 1000 --output text | grep FINDINGARNS | wc –l
0
```

Amazon Linux 2016.09

```
aws inspector list-findings --assessment-run-arns "arn:aws:inspector:us-west-2:ACCOUNT:target/0-
aiPGypOn/template/0-KQ1FrZu6/run/0-Ixqaicyh" --filter '{"severities":["High"], "agentIds":
["i-0c8c9f709dd7f7cfd"]}' --max-results 1000 --output text | grep FINDINGARNS | wc –l
0
```

Quelques conseils

- Attention aux vieilles AMI et à leurs vieux *packages*
  - Amazon Linux est bien mise à jour, mais pensez à utiliser la dernière AMI en date
- Scannez régulièrement vos instances
  - Comparez la liste des instances scannées avec la liste des instances qui tournent !
- Appliquez systématiquement les mises à jour de sécurité
  - Au redémarrage (script d'initialisation)
    - Attention : Pas dans User Data, qui n'est exécuté qu'à la création de l'instance
  - Tâche *cron* sur l'instance
  - Evénements CloudWatch programmés
  - EC2 Systems Manager
- Mettez à jour l'agent Inspector à chaque changement de noyau
  - Au redémarrage (script d'initialisation)
- Intégrez Inspector dans votre pipeline de déploiement continu

https://aws.amazon.com/blogs/compute/scheduling-ssh-jobs-using-aws-lambda/
https://aws.amazon.com/ec2/systems-manager/

Ressources complémentaires

Livres blancs AWS
https://aws.amazon.com/whitepapers/auditing-security-checklist-for-use-of-aws/
https://aws.amazon.com/blogs/security/new-whitepaper-security-at-scale-logging-in-aws/
https://aws.amazon.com/whitepapers/overview-of-risk-and-compliance/

AWS re:Invent 2015 | (SEC324) New! Introducing Amazon Inspector
https://www.youtube.com/watch?v=HjuEtMrWc_w

https://aws.amazon.com/fr/blogs/aws/scale-your-security-vulnerability-testing-with-amazon-inspector/

https://aws.amazon.com/fr/about-aws/whats-new/2016/12/amazon-ec2-systems-manager-now-offers-patch-management/

Slides et vidéos des webinaires : http://bit.ly/2hKPihB

Merci !

Julien Simon
Principal Technical Evangelist, AWS
julsimon@amazon.fr
@julsimon

Webinaires 2017 : https://attendee.gotowebinar.com/register/7239291589398918401

Lundi
- Bonnes pratiques d'authentification avec AWS IAM
- Chiffrez vos données avec AWS

Mardi
- Fireside chat avec Matthieu Bouthors et Julien Simon
- Re:Invent update 1

Mercredi
- Deep dive : Amazon Virtual Private Cloud
- Bonnes pratiques anti-DDoS

Jeudi
- Re:Invent update 2
- Gérez les incidents de sécurité avec AWS CloudTrail

Vendredi
- Automatisez vos audits de sécurité avec Amazon Inspector
- Bonnes pratiques de sécurité sur AWS

Slides et vidéos des webinaires : http://bit.ly/2hKPihB