Utilisation d'AWS Config pour surveiller la conformité de la licence sur les hôtes Amazon EC2 dédiés

Avril 2016

Mentions légales

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans avis préalable. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document ne crée pas de garanties, représentations, engagements contractuels, conditions ou assurances à l'encontre d'AWS, de ses affiliés, fournisseurs ou donneurs de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun et ne modifie aucun contrat entre AWS et ses clients.

Table des matières

Résumé 4

Introduction 4

Mise en place d'AWS Config pour assurer le suivi des hôtes dédiés et des instances EC2 5

Création d'une règle personnalisée pour vérifier que les instances lancées se trouvent sur un hôte dédié 7

Gestion des autres exigences de conformité Bring Your Own License (licences à fournir, BYOL) avec les règles d'AWS Config 14

Conclusion 15

Collaborateurs 15

Suggestions de lecture 15

Résumé

Les hôtes dédiés d'Amazon Elastic Compute Cloud (EC2) peuvent aider les entreprises à diminuer les coûts en permettant d'utiliser les licences liées au serveur existantes. De nombreux clients peuvent également utiliser les hôtes dédiés pour répondre aux exigences de conformité de l'entreprise et de réglementation. Très souvent, les clients qui utilisent les hôtes dédiés désirent enregistrer et évaluer en continu les modifications apportées à leur infrastructure, de manière à rester conformes aux termes de la licence et aux exigences réglementaires.

Ce livre blanc met en évidence les façons dont vous pouvez tirer parti d'AWS Config et des règles d'AWS Config pour contrôler la conformité des licences sur les hôtes dédiés Amazon EC2.

Introduction

Ce livre blanc indique comment vous pouvez installer AWS Config de manière à enregistrer les modifications de configuration apportées aux hôtes dédiés Amazon EC2 et aux instances EC2 afin de vérifier la conformité de votre licence. Vous découvrirez comment créer des règles AWS Config pour gérer la façon dont vos licences liées au serveur sont utilisées sur Amazon Web Services (AWS). Nous allons créer un exemple de règle qui vérifie que toutes les instances d'un compte créé à partir d'une AMI (Amazon Machine Image) appelée MyWindowsImage sont lancées sur un hôte dédié spécifique. Nous allons également décrire les autres vérifications qui peuvent être utilisées pour assurer la surveillance de la conformité avec les restrictions de licence courantes et pour gérer vos ressources en hôtes dédiés.

Un hôte dédié Amazon EC2 est un serveur physique avec une capacité d'instances EC2 à votre entière disposition. Vous bénéficiez d'une visibilité complète sur le nombre de sockets et de cœurs physiques qui prennent en charge vos instances sur un hôte dédié. Les hôtes dédiés vous permettent de placer vos instances sur un serveur physique spécifique. Ce niveau de visibilité et de contrôle vous permet d'utiliser vos licences logicielles existantes par socket, par cœur ou par machine virtuelle (VM) (par ex., Microsoft Windows Server) pour faire des économies et vous conformer aux exigences réglementaires.

Pour assurer le suivi des instances lancées, arrêtées ou résiliées sur un hôte dédié, vous pouvez utiliser AWS Config. AWS Config associe ces informations avec les informations au niveau de l'hôte et de l'instance correspondant aux licences logicielles, commel'ID de l'hôte, les ID d'AMI et le nombre de sockets et de cœurs physiques par hôte. Vous pouvez ensuite utiliser ces données pour vérifier l'utilisation par rapport à vos métriques de licence.

Vous pouvez utiliser les règles d'AWS Config pour effectuer un choix dans un ensemble de règles pré-élaborées sur la base des bonnes pratiques d'AWS ou pour définir des règles personnalisées. Vous pouvez définir des règles qui vérifient la validité des modifications apportées aux ressource suivies par AWS Config par rapport aux politiques et consignes que vous avez définies. Vous pouvez définir ces règles AWS Config afin d'évaluer chaque modification apportée à la configuration d'une ressource ou vous pouvez les exécuter à une fréquence choisie. Vous pouvez également générer vos propres règles personnalisées en créant des fonction AWS Lambda dans n'importe quelle langue prise en charge.

Mise en place d'AWS Config pour assurer le suivi des hôtes dédiés et des instances EC2

Ouvrez AWS Management Console et accédez à la console EC2. Sur la page Hôtes dédiés EC2, observez le bouton **Modifier l'enregistrement de la configuration** disponible en haut. L'icône en **rouge** indique qu'AWS Config n'est actuellement pas configuré pour enregistrer les modifications de configuration apportées aux hôtes dédiés et aux instances.

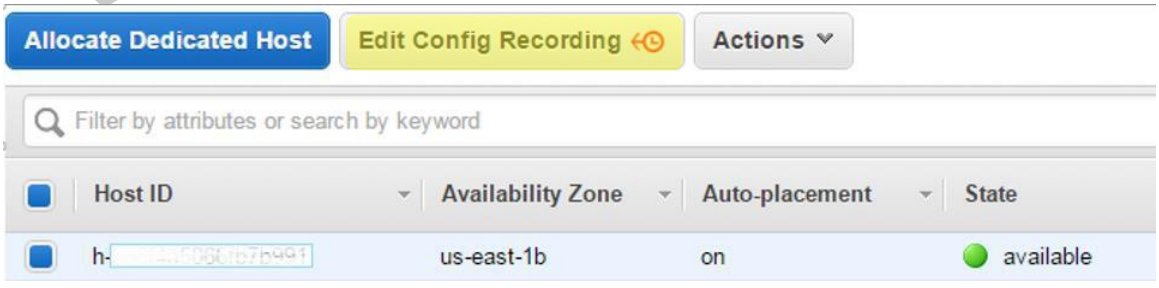

Figure 1 : Bouton Modifier l'enregistrement de la configuration avec l'icône rouge sur la console de l'hôte dédié

La mise en route d'AWS Config est simple. Cliquez sur le bouton **Modifier l'enregistrement de la configuration** pour ouvrir la page des paramètres d'AWS Config. Dans cette page, cochez la case **Enregistrer toutes les ressources prises en charge dans cette région**.

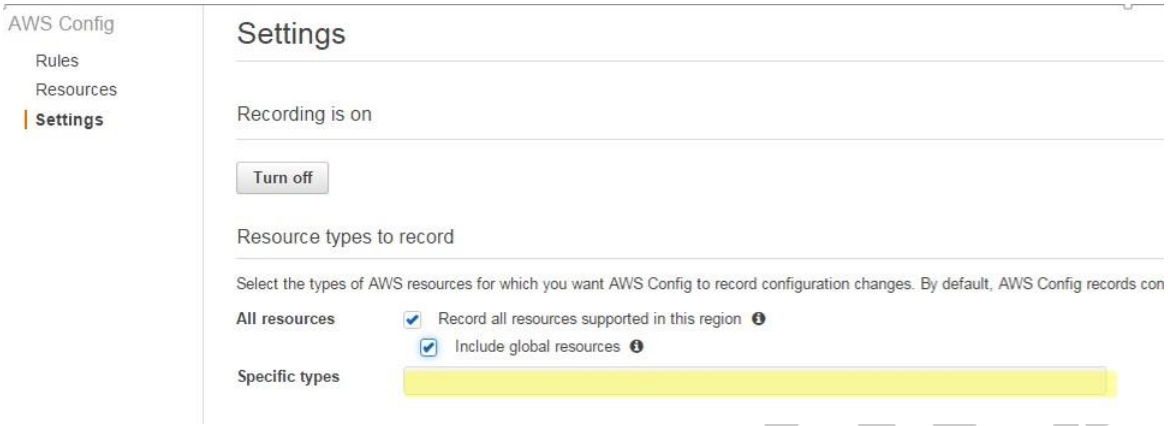

Figure 2 : Sélection des types de ressources à enregistrer sur la page d'AWS Config

Vous pouvez choisir d'activer l'enregistrement uniquement pour les hôtes dédiés et les instances en sélectionnant ces ressources dans le champ **Types spécifiques**. Si vous paramétrez AWS Config pour la première fois, vous devez indiquer un compartiment Amazon S3 dans lequel AWS Config peut déposer l'historique de configuration et les fichiers d'instantané. Vous pouvez aussi, de manière facultative, indiquer une rubrique Amazon Simple Notification Service (SNS) dans laquelle les notifications de modification et de conformité seront déposées. Enfin, il vous sera demandé d'accorder les autorisations appropriées pour AWS Config et d'enregistrer les paramètres. Pour plus de détails sur le paramétrage d'AWS Config à l'aide d'AWS Management Console ou de la CLI, consultez la documentation intitulée Mise en route d'AWS Config.

Une fois le paramétrage d'AWS Config terminé, vous remarquerez que l'icône de la page de la console EC2 pour les hôtes dédiés est devenue **verte**. Ceci signifie qu'AWS Config enregistre les modifications de configuration apportées à l'ensemble des instances EC2 et aux hôtes dédiés.

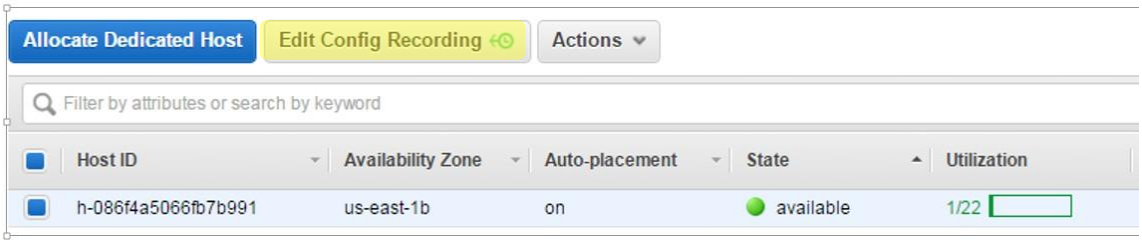

Figure 3 : Bouton Modifier l'enregistrement de la configuration avec l'icône verte

Création d'une règle personnalisée pour vérifier que les instances lancées se trouvent sur un hôte dédié

Maintenant que vous avez paramétré AWS Config de manière à démarrer l'enregistrement des modifications de configuration apportées aux hôtes dédiés et aux instances EC2, vous pouvez commencer à rédiger des règles permettant d'évaluer l'état de conformité de la licence de toutes les instances du compte. Pour débuter, vous allez rédiger une règle qui vérifie que toutes les instances lancées à partir de l'AMI MyWindowsImage sont placées sur un hôte dédié spécifique. Dans le cadre de cet exemple, nous supposons que MyWindowsImage est le nom d'une AMI que vous avez importée et qu'il s'agit de l'image de la machine d'une licence Microsoft Server que vous détenez.

Avant de créer une règle, inspectez d'abord les instances et les hôtes dédiés de votre compte : recherchez les types de ressources **Instance EC2** et **Hôte EC2**. La figure 4 présente un hôte dédié et un certain nombre d'instances.

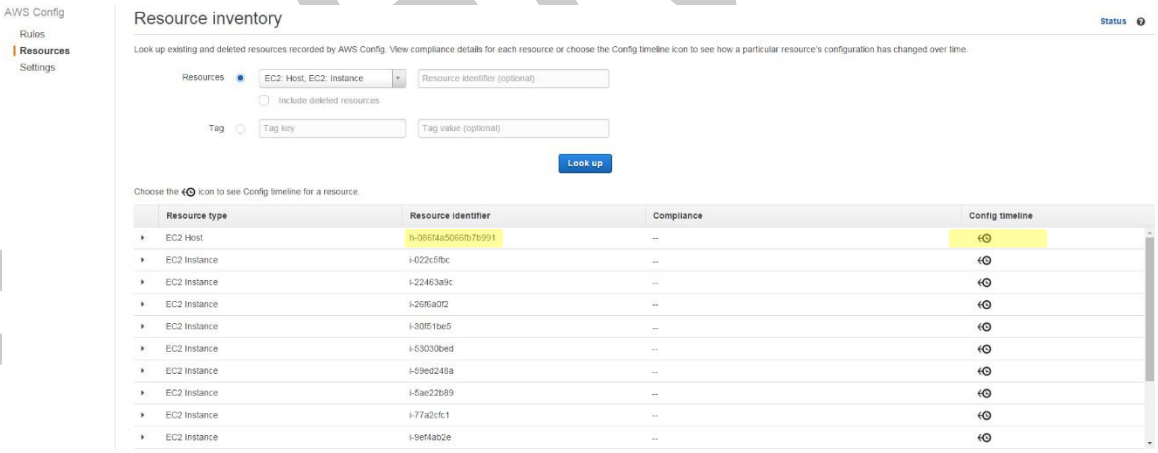

Figure 4 : Examen de l'inventaire des ressources

Cliquez sur l'icône de l'hôte dédié pour accéder à la Chronologie de configuration de manière à visualiser la configuration de l'hôte dédié, avec les sockets, les cœurs, le total des processeurs virtuels et les processeurs virtuels disponibles. Vous pouvez également visualiser toutes les instances actuellement exécutées sur l'hôte. En parcourant la chronologie, vous pouvez connaître toutes les configurations historiques de l'hôte dédié, y compris les instances qui ont été lancées sur l'hôte dédié par le passé. Vous pouvez également observer la Chronologie de configuration de chacune de ces instances.

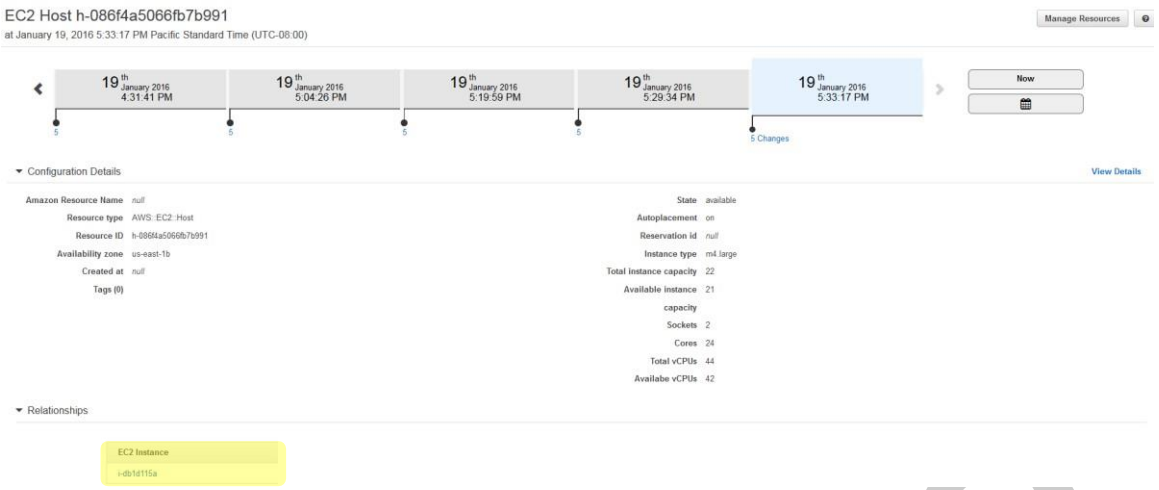

Figure 5 : Chronologie de l'historique de configuration des ressources de Config

Vous définissez ensuite la nouvelle règle dans AWS Config et rédigez la fonction AWS Lambda pour la règle. Pour cela, cliquez sur **Ajouter une règle** dans la console AWS Config, puis cliquez sur **Créer une fonction AWS Lambda** pour définir la fonction à exécuter.

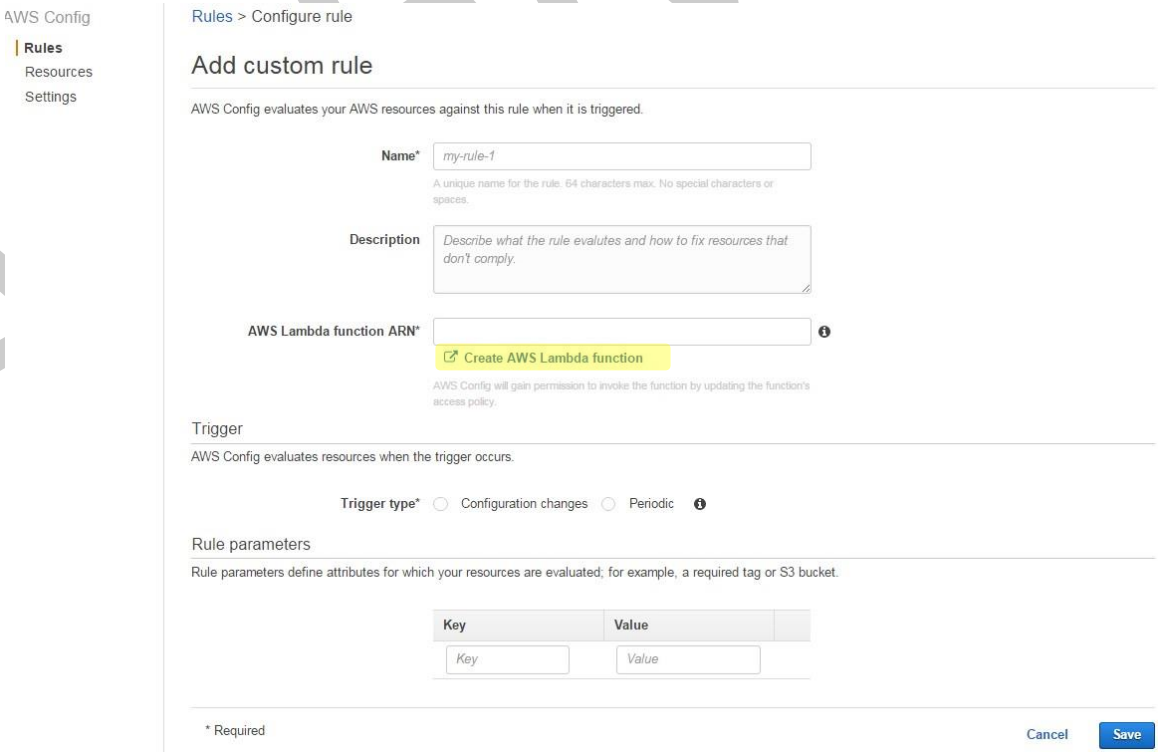

Figure 6 : Page de création d'une règle AWS Config

Dans la console Lambda, sélectionnez le plan `config-rule-change-triggered` pour commencer.

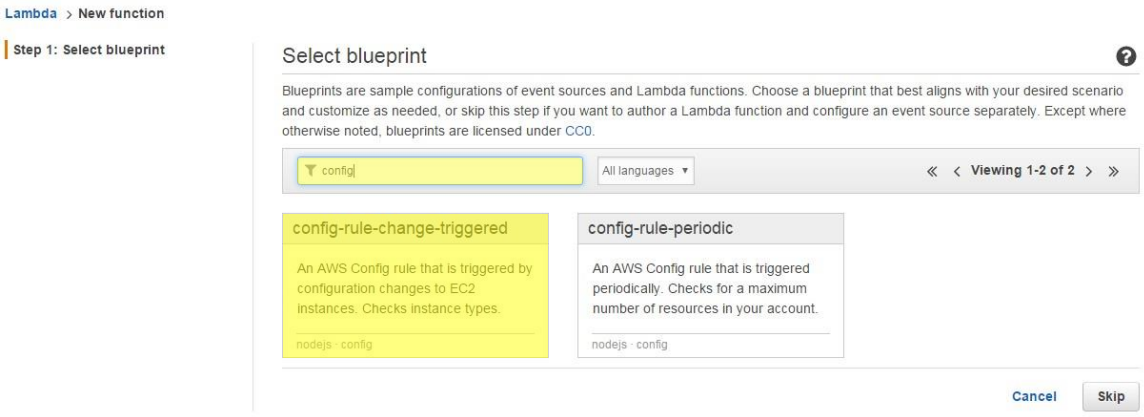

Figure 7 : Page de sélection du plan Lambda

Vous pouvez annoter les états de conformité. Pour cela, ajoutez tout d'abord une variable globale appelée `annotation`.

```
var aws = require('aws-sdk');
var config = new aws.ConfigService();
var annotation;
```

Vous devez également modifier la fonction `evaluateCompliance` et le gestionnaire appelé par AWS Lambda. Le reste du code du plan peut rester tel qu'il est.

```
function evaluateCompliance(configurationItem, ruleParameters, context)
   { checkDefined(configurationItem, "configurationItem");
   checkDefined(configurationItem.configuration,
"configurationItem.configuration");
   checkDefined(ruleParameters, "ruleParameters");

   if ('AWS::EC2::Instance' !== configurationItem.resourceType)
      { return 'NOT_APPLICABLE';
   }

   if (ruleParameters.imageId === configurationItem.configuration.imageId
```

```
&& ruleParameters.hostId !==
configurationItem.configuration.placement.hostId) {
    annotation = "Instance " + configurationItem.configuration.instanceId
                    + " launched from BYOL AMI " +
    configurationItem.configuration.imageId
                    + " has not been placed on dedicated host " +
    ruleParameters.hostId;

     return 'NON_COMPLIANT';
  }
  else {
     return 'COMPLIANT';
  }
```

Pour cet exemple de fonction, `imageId` et `hostId` sont des paramètres communiqués à la fonction par la règle AWS Config qui sera créée par la suite. Le paramètre `imageId` contiendra l'ID de l'AMI de MyWindowsImage. Utilisez ce paramètre pour identifier les instances lancées à partir de cette image. Une fois que vous avez détecté qu'une instance a été lancée à partir de MyWindowsImage, vous pouvez alors vérifier si l'instance a été lancée sur l'hôte dédié indiqué et identifié par le paramètre `hostId`. L'instance est marquée comme non conforme s'il s'avère qu'elle ne s'exécute pas sur l'hôte sur lequel toutes les instances lancées à partir de MyWindowsImage doivent s'exécuter.

Vous pouvez annoter les états de conformité d'une ressource avec d'autres informations indiquant pourquoi la ressource a été signalée comme non conforme. Cet exemple détaille la raison pour laquelle l'instance a été marquée comme non conforme et attribue ce texte à la variable globale `annotation`. Enfin, les modifications sont apportées au gestionnaire afin de communiquer l'annotation avec le reste des informations de conformité.

```
putEvaluationsRequest.Evaluations = [
  {
    ComplianceResourceType: configurationItem.resourceType,
    ComplianceResourceId: configurationItem.resourceId,
    ComplianceType: compliance,
    OrderingTimestamp: configurationItem.configurationItemCaptureTime,
    Annotation: annotation
  }
];
```

Une fois les modifications apportées à la fonction AWS Lambda, sélectionnez le rôle approprié et enregistrez la fonction. Dans notre exemple, nous avons également noté l'Amazon Resource Name (ARN) de la fonction. Une fois la fonction créée, revenez à la console AWS Config et entrez l'ARN de la fonction que vous venez de créer.

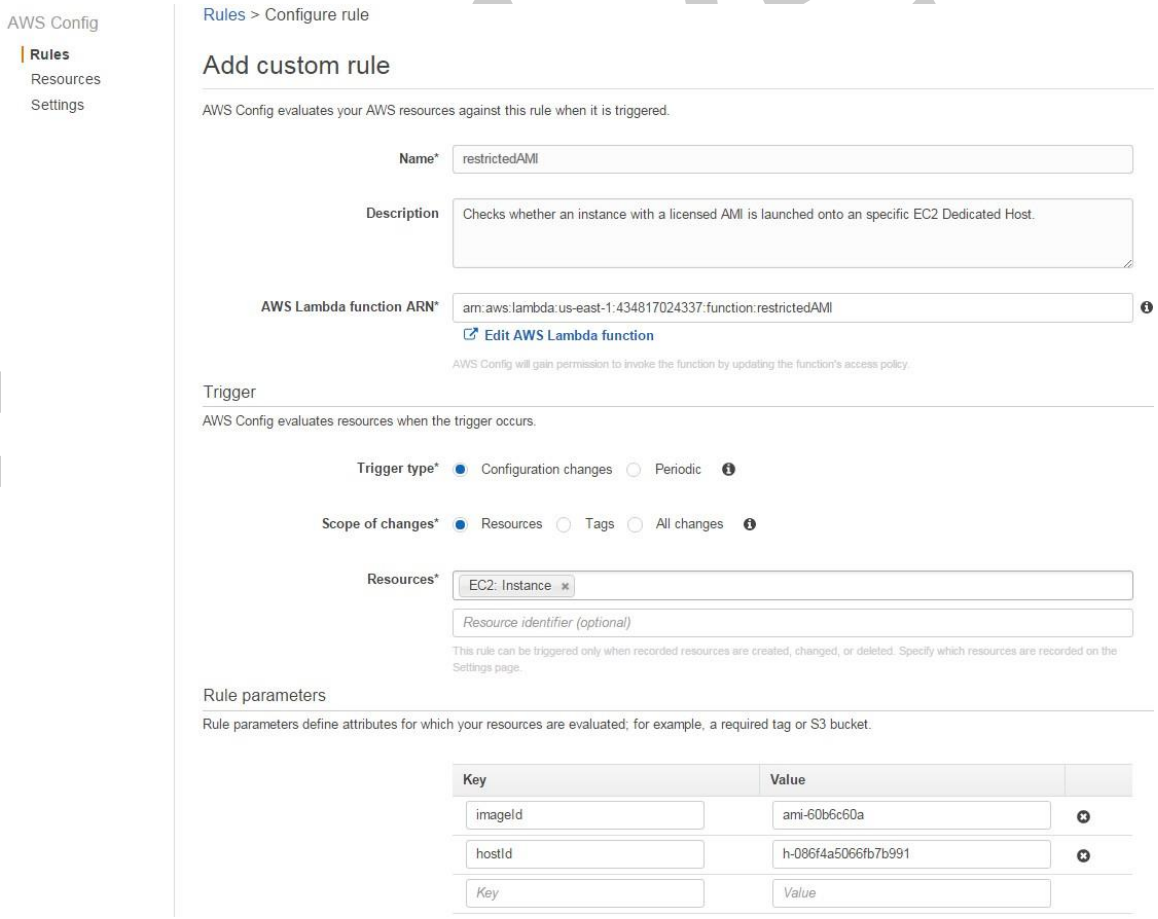

Figure 8 : Saisie de l'ARN de la fonction AWS Lambda sur la page de création de la règle AWS Config

Une fois les paramètres adaptés à la règle indiqués, enregistrez-la. La règle est évaluée une fois immédiatement après sa création, puis après toute modification apportée aux instances EC2. Dans cet exemple, les deux instances ont été lancées à partir de MyWindowsImage, mais une seule a été lancée sur l'hôte dédié désigné. La règle d'AWS Config marque l'autre instance comme non conforme.

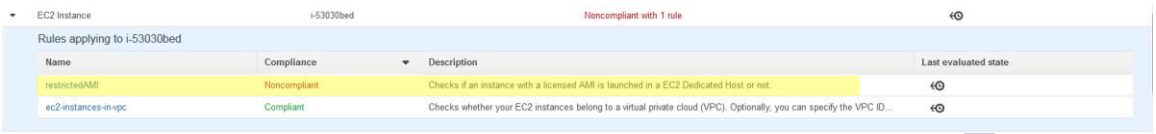

Figure 9 : Instance marquée comme non conforme

L'état **Conforme** ou **Non conforme** pour chaque règle est également envoyé sous forme de notification via la rubrique Amazon SNS que vous avez créée lorsque vous avez défini AWS Config. Vous pouvez configurer ces notifications de manière à envoyer un e-mail, déclencher une action corrective ou enregistrer un ticket. La notification Amazon SNS contient des détails sur la modification de l'état de conformité, y compris l'annotation qui détaille le motif de non-conformité.

Affichez la chronologie de cette ressource dans AWS Config Management Console :
https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::EC2::Instance/i-a46d7125?time=2016-01-28T02:02:35.606Z

Enregistrement de la modification de nouvelle conformité :

{
 "awsAccountId": "434817024337",
 "configRuleName": "restrictedAMI",
 "configRuleARN": "arn:aws:config:us-east-1:434817024337:config-rule/config-rule-hz8yxz",
 "resourceType": "AWS::EC2::Instance",
 "resourceId": "i-a46d7125",
 "awsRegion": "us-east-1",
 "newEvaluationResult": {
  "evaluationResultIdentifier": {
   "evaluationResultQualifier": {
    "configRuleName": "restrictedAMI",
    "resourceType": "AWS::EC2::Instance",
    "resourceId": "i-a46d7125"
   },
   "orderingTimestamp": "2016-01-28T02:02:35.606Z"
  },
  "complianceType": "NON_COMPLIANT",
  "resultRecordedTime": "2016-01-28T02:02:41.417Z",
  "configRuleInvokedTime": "2016-01-28T02:02:40.396Z",
  "annotation": "Instance i-a46d7125 launched from BYOL AMI ami-60b6c60a has not been placed on dedicated host h-086f4a5066fb7b991",
  "resultToken": null
 },
 "oldEvaluationResult": {
  "evaluationResultIdentifier": {
   "evaluationResultQualifier": {
    "configRuleName": "restrictedAMI",
    "resourceType": "AWS::EC2::Instance",
    "resourceId": "i-a46d7125"
   },
   "orderingTimestamp": "2016-01-28T01:44:54.553Z"
  },
  "complianceType": "COMPLIANT",
  "resultRecordedTime": "2016-01-28T01:45:03.438Z",
  "configRuleInvokedTime": "2016-01-28T01:45:01.298Z",
  "annotation": null,
  "resultToken": null
 },
 "notificationCreationTime": "2016-01-28T02:02:42.317Z", "messageType":
 "ComplianceChangeNotification", "recordVersion": "1.0"
}

Gestion des autres exigences de conformité Bring Your Own License (licences à fournir, BYOL) avec les règles d'AWS Config

La règle d'AWS Config créée dans l'exemple ci-dessus vérifie une des nombreuses exigences de conformité que vous pouvez avoir associées aux licences BYOL liées au serveur. Cette règle peut être étendue de manière à vérifier les autres restrictions spécifiques à la licence, comme les restrictions suivantes :

- Affinité de l'hôte des instances
- Nombre de sockets ou nombre de cœurs de l'hôte dédié sur lequel les instances sont lancées
- Durée pendant laquelle une instance doit se trouver sur un hôte dédié désigné

En outre, vous pouvez également surveiller l'utilisation des hôtes dédiés que vous possédez et les marquer comme non conformes si leur utilisation chute au-dessous d'un certain seuil. Ceci vous permet d'optimiser votre flotte d'hôtes dédiés.

Conclusion

Dans ce livre blanc, vous avez appris comment utiliser AWS Config conjointement aux règles d'AWS Config afin de vérifier la conformité de votre licence sur les hôtes dédiés Amazon EC2. AWS Config peut être plus largement utilisé pour surveiller et gérer toutes vos ressources. Pour plus d'informations, consultez la rubrique Suggestions de lecture, ci-dessous.

Collaborateurs

Les personnes et organisations suivantes ont participé à l'élaboration de ce document :

- Chayan Biswas, responsable produit senior, AWS Config

Suggestions de lecture

Pour obtenir de l'aide, consultez les ressources suivantes :

- Documentation sur ce qu'AWS Config prend en charge : Ressources prises en charge, Eléments de configuration et Relations
- Billet de blog : Comment enregistrer et gérer les configurations de vos ressources IAM Utilisation d'AWS Config
- Page de produit d'AWS Config : AWS Config